February 23, 2023

FACT SHEET*

Call Authentication Trust Anchor

Sixth Report and Order and Sixth Further Notice of Proposed Rulemaking – WC Docket No. 17-97

Background: Protecting Americans from unwanted and illegal robocalls remains the Commission's top consumer protection priority. One key component in this fight is the STIR/SHAKEN caller ID authentication framework, which helps protect consumers from illegally spoofed robocalls by verifying that the caller ID information transmitted with a particular call matches the caller's telephone number. The effectiveness of the STIR/SHAKEN framework increases with more widespread adoption and implementation within our communications networks. For that reason, in May 2022, we required gateway providers—intermediate providers that are the point of entry for foreign calls into the United States—to implement STIR/SHAKEN, and sought comment on ways to expand STIR/SHAKEN requirements to other intermediate providers in the call path, as well as several other measures to better protect American consumers from illegal robocalls. This *Sixth Report and Order* would close a critical gap in the STIR/SHAKEN framework by requiring intermediate providers that receive unauthenticated calls directly from domestic originating providers to authenticate those calls. In addition, it would expand robocall mitigation requirements for all providers, adopt more robust enforcement tools, and define the STIR/SHAKEN obligations of satellite voice service providers. The *Sixth Further Notice of Proposed Rulemaking* would seek comment on additional steps to further enhance the effectiveness of the STIR/SHAKEN caller ID authentication regime.

What the *Sixth Report and Order* Would Do:

- Require intermediate providers that receive unauthenticated Session Initiation Protocol (SIP) calls directly from originating providers to authenticate those calls using STIR/SHAKEN.
- Require all providers, regardless of their STIR/SHAKEN implementation status, to take "reasonable steps" to mitigate illegal robocall traffic and submit a certification and mitigation plan to the Commission's Robocall Mitigation Database.
- Require all providers to submit additional information with their certifications to the Commission's Robocall Mitigation Database, including details on their role in the call chain, STIR/SHAKEN implementation obligations, and any recent formal law enforcement or regulatory investigation into suspected unlawful robocalling.
- Prohibit downstream providers from accepting traffic from intermediate providers not listed in the Commission's Robocall Mitigation Database.
- Establish new enforcement tools to hold illegal robocallers accountable for violations of our rules, including additional penalties for noncompliance and an expedited removal procedure for facially deficient Robocall Mitigation Database filings.
- Grant an ongoing STIR/SHAKEN implementation extension for satellite providers that are small service providers using North American Numbering Plan numbers to originate calls.

What the *Sixth Further Notice of Proposed Rulemaking* Would Do:

- Seek further comment on the use of third-party caller ID authentication solutions and whether any changes should be made to the Commission's rules to permit, prohibit, or limit their use.
- Seek comment on whether to eliminate the STIR/SHAKEN implementation extension for voice service providers that cannot obtain a Service Provider Code token.

* This document is being released as part of a "permit-but-disclose" proceeding. Any presentations or views on the subject expressed to the Commission or its staff, including by email, must be filed in WC Docket No. 17-97, which may be accessed via the Electronic Comment Filing System (https://www.fcc.gov/ecfs/). Before filing, participants should familiarize themselves with the Commission's ex parte rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. See 47 CFR § 1.1200 et seq.

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	

SIXTH REPORT AND ORDER AND FURTHER NOTICE OF PROPOSED RULEMAKING*

Adopted: [] **Released: []**

Comment Date: 30 days after date of publication in the Federal Register
Reply Comment Date: 60 days after date of publication in the Federal Register

By the Commission:

TABLE OF CONTENTS

* This document has been circulated for tentative consideration by the Commission at its March open meeting. The issues referenced in this document and the Commission's ultimate resolution of those issues remain under consideration and subject to change. This document does not constitute any official action by the Commission. However, the Chairwoman has determined that, in the interest of promoting the public's ability to understand the nature and scope of issues under consideration, the public interest would be served by making this document publicly available. The FCC's ex parte rules apply and presentations are subject to "permit-but-disclose" ex parte rules. See, e.g., 47 C.F.R. §§ 1.1206, 1.1200(a). Participants in this proceeding should familiarize themselves with the Commission's ex parte rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. See 47 CFR §§ 1.1200(a), 1.1203.

I. INTRODUCTION

1. Protecting Americans from the consequences of unwanted and illegal robocalls remains the Commission's top consumer protection priority. We receive more complaints about unwanted calls, including illegal robocalls, than any other issue, with approximately 119,000 complaints submitted in 2022 alone.[1] The Federal Trade Commission (FTC) reports that 36% of the fraud reports that it received in 2021 had a phone call as the contact method, with approximately $692 million defrauded from consumers due to these calls.[2] That amount is a fraction of the $13.5 billion that the Commission has estimated is lost by consumers due to illegal robocalls,[3] which does not account for the non-quantifiable losses suffered by consumers such as lost time and eroded confidence in the nation's telephone network.[4]

2. The Commission has worked diligently to combat the scourge of robocalls on multiple fronts.[5] One key component in that fight is the STIR/SHAKEN caller ID authentication framework, which protects consumers from illegally spoofed robocalls by verifying that the caller ID information

[1] The Commission received approximately 193,000 such complaints in 2019, 157,000 in 2020, 164,000 in 2021, and 119,000 in 2022. FCC, *Consumer Complaint Data Center*, https://www.fcc.gov/consumer-help-center-data (last visited Jan. 31, 2023).

[2] FTC, Consumer Sentinel Network Data Book 2021 at 12 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf.

[3] *See Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources*, 35 FCC Rcd 3241, 3263, paras. 47-48 (2020) (*First Caller ID Authentication Report and Order and Further Notice*).

[4] *See id.*

[5] For example, in enforcement actions, the Commission has taken action to mitigate the impact of robocalls associated with student loan debt and auto warranty scams. *See Urth Access, LLC*, File No. EB-TCD-22-00034232, Order, DA 22-1271 (EB Dec. 8, 2022), https://docs.fcc.gov/public/attachments/DA-22-1271A1.pdf (directing all U.S.-based voice service providers to take immediate steps to mitigate suspected illegal student loan-related scam robocall traffic); *Sumco Panama SA et al.*, Notice of Apparent Liability for Forfeiture, FCC 22-99, at 16, 32, paras. 36, 72 (Dec. 23, 2022) (proposing a forfeiture of $299,997,000 against providers associated with auto warranty scam robocalls). In October 2022, the Enforcement Bureau adopted orders to begin the process of removing seven providers from the Robocall Mitigation Database for failing to identify steps taken to avoid serving as the origination point of illegal robocall traffic. Press Release, Federal Communications Commission, FCC Plans to Remove Companies from Key Database for Non-Compliance with Anti-Robocall Rules (Oct. 3, 2022), https://www.fcc.gov/document/fcc-remove-companies-robocall-database-non-compliance. The FCC has also entered into Memoranda of Understanding with 44 state jurisdictions, the District of Columbia, and Guam to establish critical information sharing and cooperation regarding robocalls. *See* FCC, *State Robocall Investigation Partnerships*, https://www.fcc.gov/fcc-state-robocall-investigation-partnerships (last updated Feb. 17, 2023); Press Release, Federal Communications Commission, FCC Chairwoman and Illinois Attorney General Announce Robocall Enforcement Partnership (Feb. 17, 2023), https://docs.fcc.gov/public/attachments/DOC-391161A1.pdf.

transmitted with a particular call matches the caller's telephone number.[6] While the caller ID authentication technology used in the STIR/SHAKEN framework is effective as designed,[7] its overall success in curtailing illegally spoofed robocalls depends on broad implementation by providers. Accordingly, in this *Sixth Report and Order*, we continue to strengthen and expand caller ID authentication requirements in the STIR/SHAKEN ecosystem by requiring non-gateway intermediate providers that receive unauthenticated calls directly from an originating provider to use STIR/SHAKEN to authenticate those calls.

3. Further, with this *Sixth Report and Order*, we expand robocall mitigation requirements for all providers, including those that have not yet implemented STIR/SHAKEN because they lack the necessary infrastructure or are subject to an implementation extension. We empower the Enforcement Bureau with new tools and penalties to hold providers accountable for failing to comply with our rules. We also define the STIR/SHAKEN obligations of satellite providers. Finally, we adopt a *Sixth Further Notice of Proposed Rulemaking* to seek comment on additional measures that may strengthen and expand the Commission's caller ID authentication regime and stem the tide of illegally spoofed robocalls.

II. BACKGROUND

A. The STIR/SHAKEN Caller ID Authentication Framework

4. The STIR/SHAKEN caller ID authentication framework[8] protects consumers from illegally spoofed robocalls by enabling authenticated caller ID information to securely travel with the call itself throughout the entire call path.[9] The Commission, consistent with Congress's direction in the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act,[10] adopted rules requiring voice service providers[11] to implement STIR/SHAKEN in the IP portions of their voice

[6] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Fourth Report and Order, 36 FCC Rcd 17840, para. 1 (2021) (*Small Provider Order*). Call "spoofing" is a practice that involves falsifying caller ID information in order to trick unsuspecting Americans into thinking that calls are trustworthy because the caller ID information appears as if the call came from a neighbor or a familiar or reputable source. *See Call Authentication Trust Anchor, Appeals of the STIR/SHAKEN Governance Authority Token Revocation Decisions*, WC Docket Nos. 17-97 and 21-291, Third Report and Order, 36 FCC Rcd 12878, para. 1 (2021).

[7] FCC, Triennial Report on the Efficacy of the Technologies Used in the STIR/SHAKEN Caller ID Authentication Framework at 9-11 (Dec. 30, 2022), https://www.fcc.gov/document/triennial-report-efficacy-stirshaken (*Triennial STIR/SHAKEN Report*).

[8] The STIR/SHAKEN framework is a set of technical standards and protocols that enable providers to authenticate and verify caller ID information transmitted with Session Initiation Protocol (SIP) calls. A working group of the Internet Engineering Task Force (IETF) called the Secure Telephony Identity Revisited (STIR) developed several protocols for authenticating caller ID information. The Alliance for Telecommunications Industry Solutions (ATIS), in conjunction with the SIP Forum, produced the Signature-based Handling of Asserted information using toKENs (SHAKEN) specification, which standardizes how the protocols produced by STIR are implemented across the industry. *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1862-63, para. 7 (2020) (*Second Caller ID Authentication Report and Order*).

[9] *See id.* at 1862, para. 6.

[10] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105 (2019) (codified in 47 U.S.C. § 227b) (TRACED Act).

[11] Because the TRACED Act defines "voice service" in a manner that excludes intermediate providers, our authentication and Robocall Mitigation Database rules use "voice service provider" in this manner. *See* 47 U.S.C. § 227b(a)(2)(A); 47 CFR § 64.6300(n) (defining voice service as "any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end-user using resources from the North American Numbering Plan or any successor"). Our rules in 47 CFR § 64.1200, many of which the Commission adopted prior to adoption of the TRACED Act, use a definition of "voice service provider" that includes intermediate providers. In that context, use of the TRACED Act definition of "voice service" would create inconsistency with our existing rules. *See, e.g.*, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, (continued….)

networks by June 30, 2021,[12] subject to certain exceptions.[13]

5. The STIR/SHAKEN framework consists of two components: (1) the technical process of authenticating and verifying caller ID information; and (2) the certificate governance process that maintains trust in the caller ID authentication information transmitted along with a call.[14] The first component relies on public key cryptography to securely transmit the information that an originating voice service provider knows about the caller and its relationship to the phone number it is using along with the call itself, allowing the terminating voice service provider to verify the information on the other end.[15] This encrypted information is contained in a unique part of the SIP message known as the "Identity" header field.[16] After the originating voice service provider authenticates this caller ID information for a particular call and adds this information, it travels along with the call from the originating voice service provider, through any intermediate providers, and then to the terminating voice service provider.[17] When the terminating voice service provider receives the call with the Identity header attached, it can decrypt it, verify the caller ID information, and then use that information, along with other information, to protect its subscribers from unwanted and illegal calls.[18]

6. The second component relies on digital certificates issued to a provider through a neutral governance system to maintain trust and accountability among providers.[19] The provider first obtains a Service Provider Code (SPC) token from the STIR/SHAKEN Policy Administrator and then presents that token to a STIR/SHAKEN Certificate Authority to obtain a certificate, which states, in essence, that the provider is the entity it claims to be and that it has the right to authenticate the caller ID information.[20] This system is overseen by a Governance Authority—a role filled by an entity called the Secure Telephone Identity Governance Authority[21]—which establishes the policies and procedures regarding how providers may acquire and maintain certificates.[22] The Policy Administrator applies the rules set by the Governance Authority,[23] and third-party Certification Authorities (themselves subject to Policy

(Continued from previous page)
CG Docket No. 17-59, Fourth Report and Order, 35 FCC Rcd 15221, 15222 n.2 (2020) (*Fourth Call Blocking Order*). To avoid confusion, for purposes of this item, we use the term "voice service provider" consistent with the TRACED Act definition and where discussing caller ID authentication or the Robocall Mitigation Database. In all other instances, we use "provider" and specify the type of provider as appropriate. Unless otherwise specified, we mean any provider, regardless of its position in the call path.

[12] 47 CFR § 64.6301; *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3252, para. 24.

[13] 47 CFR §§ 64.6304, 64.6306; *see also Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1876-83, paras. 36-51.

[14] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1862-63, para. 7.

[15] *Id.* at 1863, para. 8.

[16] *Id.*

[17] *See id.*

[18] *See First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3244-45, para. 6. For example, caller ID authentication information may be incorporated with other analytics to determine whether a call should be blocked under our existing safe harbors for call blocking. *See* 47 CFR § 64.1200(k)(3), (11).

[19] *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3246, para. 9.

[20] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1864, para. 11.

[21] *Id.* at 1864, para. 11; *see also* Secure Telephone Identity Governance Authority (STI-GA), *STI Governance Authority*, https://sti-ga.atis.org (last visited Nov. 25, 2022).

[22] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1864, para. 11.

[23] *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3246, para. 10. The role of (continued….)

Administrator approval)[24] issue the digital certificates to providers.[25] This robust system of checks and balances ensures that providers can trust one another based on the certificates transmitted along with STIR/SHAKEN-authenticated calls.

7. The Commission requires voice service providers subject to a STIR/SHAKEN implementation extension—including facilities-based small voice service providers[26] and voice service providers with non-IP technology—to adopt and implement robocall mitigation practices in lieu of caller ID authentication.[27] To comply with this requirement, mitigation programs must include "detailed practices that can reasonably be expected to significantly reduce" either the carrying and processing (for gateway providers) or the origination (for voice service providers) of illegal robocalls.[28] The provider must "comply with the practices its plan requires," and its program will be deemed insufficient if it "knowingly or through negligence" carries or processes (for gateway providers) or originates (for voice service providers) calls for illegal robocall campaigns.[29] Providers subject to an implementation extension must commit to responding "fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocalls that use its service to originate calls."[30] In adopting

(Continued from previous page)
Policy Administrator is currently held by iconectiv. *See* iconectiv, *Industry Players*, https://authenticate.iconectiv.com/industry-players (last visited Feb. 1, 2023).

[24] *See First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3246, para. 10. The Policy Administrator has approved 9 certification authorities. *See* iconectiv, *Approved Certification Authorities*, https://authenticate.iconectiv.com/approved-certification-authorities (last visited Feb. 16, 2023).

[25] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1864, para. 11. Under the current Governance Authority rules, a provider must meet certain requirements to receive a certificate. *See* STI-GA, Policy Decision Binder Version 4.1, Policy Decision 001: SPC Token Access Policy Version 1.2, at 5 (Oct. 29, 2021), https://sti-ga.atis.org/wp-content/uploads/sites/14/2022/12/221025-STIGA-Board-Policy-Decision-Binder-v4-1-Final-1.pdf. To obtain a token, the Governance Authority policy requires that a provider must "(1) [h]ave a current form 499A on file with the FCC . . . ; (2) [h]ave been assigned an Operating Company Number (OCN) . . . ; [and] (3) [h]ave certified with the FCC that they have implemented STIR/SHAKEN or comply with the [Commission's] Robocall Mitigation Program requirements and are listed in the FCC [Robocall Mitigation Database], or . . . has direct access to telephone numbers from the Toll-Free Number Administrator (TFNA)." *Id*.

[26] Non-facilities-based small voice service providers were required to fully implement STIR/SHAKEN in the IP portions of their networks by June 30, 2022, and "facilities-based" providers have been granted an implementation extension until June 30, 2023. *See* 47 CFR § 64.6304(a)(1) (providing an extension of the implementation deadline for small voice service providers); *id.* § 64.6304(a)(1)(i) (limiting the extension for non-facilities-based small voice service providers to June 30, 2022).

[27] 47 CFR §§ 64.6304, 64.6305; *see also Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1876-83, 1897-907, paras. 36-51, 74-94.

[28] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1900, para. 78 (obligation for voice service providers); *see also Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Sixth Report and Order, Fifth Report and Order, Order on Reconsideration, Order, Seventh Further Notice of Proposed Rulemaking, Fifth Further Notice of Proposed Rulemaking, FCC 22-37, at 43-44, para. 103 (2022) (obligation for gateway providers) (*Gateway Provider Order* or *Fifth Caller ID Authentication Further Notice*).

[29] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1900, para. 78 (obligation for voice service providers); *Gateway Provider Order* at 44, para. 103 (obligation for gateway providers).

[30] 47 CFR § 64.6305(a)(2). Congress required the Commission to select a single consortium to "conduc[t] private-led efforts to trace back the origin of suspected unlawful robocalls." TRACED Act § 13(d)(1). Pursuant to this directive, the Commission's Enforcement Bureau selected the Industry Traceback Group (ITG) as the industry traceback consortium. *See Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, EB Docket No. 20-22, Report and Order, 35 FCC Rcd 7886, 7889, para. 10 (EB 2020). All providers, regardless of whether they are subject to an implementation extension, are (continued….)

this requirement, the Commission explained that, if it determined that its standards-based approach to mitigation was not sufficient, it would "not hesitate to revisit the obligations we impose through rulemaking at the Commission level."[31]

8. Voice service providers were required, by June 30, 2021, to submit a certification to the Robocall Mitigation Database stating whether they had implemented STIR/SHAKEN on all or part of their networks, or not at all, and, if they had not fully implemented STIR/SHAKEN, describe their robocall mitigation program and "[t]he specific reasonable steps the voice service provider has taken to avoid originating illegal robocall traffic."[32] The Commission prohibited intermediate providers[33] and terminating voice service providers from accepting calls directly from a domestic voice service provider if that voice service provider has not filed in the Robocall Mitigation Database.[34] As of April 11, 2023, domestic providers are also prohibited from accepting calls carrying U.S. North American Numbering Plan (NANP) numbers from a foreign originating or foreign intermediate provider if the foreign provider has not filed in the Robocall Mitigation Database.[35]

9. In addition to placing these obligations on voice service providers, the Commission required intermediate providers to implement STIR/SHAKEN in their IP networks. In the *Second Caller ID Authentication Report and Order*, the Commission required intermediate providers with IP networks to pass authenticated caller ID information unaltered to the next provider in the call path[36] and either

(Continued from previous page)
currently required to respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium fully and in a timely manner, and gateway providers must respond within 24 hours. 47 CFR § 64.1200(n)(1).

[31] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1902, para. 81.

[32] 47 CFR § 64.6305(c)(1)-(2). As of February 16, 2022, 6,848 voice service providers have filed in the Robocall Mitigation Database: 2,365 attest to full STIR/SHAKEN implementation; 1,536 state that they have implemented a mix of STIR/SHAKEN and robocall mitigation; and 2,947 state that they rely solely on robocall mitigation. FCC, Robocall Mitigation Database, https://fccprod.servicenowservices.com/rmd?id=rmd_listings (last visited Feb. 16, 2023)

[33] 47 CFR § 64.6300(g) (defining an "intermediate provider" as "any entity that carries or processes traffic that traverses or will traverse the public switched telephone network at any point insofar as that entity neither originates nor terminates that traffic").

[34] *See* 47 CFR § 64.6305(e)(1); *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1904, para. 86.

[35] 47 CFR § 64.6305(e)(2); *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1904, para. 87; *Wireline Competition Bureau Announces Deadlines for Gateway Provider Robocall Mitigation Requirements and Additional Compliance Dates and Filing Instructions*, WC Docket No. 17-97, Public Notice, DA 22-1303, at 4 (WCB Dec. 12, 2022); *see also* 47 CFR § 64.6300(c) (defining foreign voice service provider). An earlier version of this prohibition was stayed while the Commission examined whether it should be modified. *See Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-.97, 36 FCC Rcd 14971, 15007-08, para. 106 (*Gateway Provider Further Notice*). The Commission adopted the current prohibition in the *Gateway Provider Order. See Gateway Provider Order* at 50, para. 122. The Commission emphasized that these rules did not constitute the exercise of jurisdiction over foreign voice service providers. *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1910, para. 99 n.370. Because the rules did not require foreign voice service providers to submit a certification into the Robocall Mitigation Database, they did not have an impermissible, direct effect on foreign voice service providers. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1910, para. 99 n.370; *Gateway Provider Order* at 49-50, para. 120 & n.354.

[36] 47 CFR § 64.6302(a). The Commission created two exceptions from this rule under which an intermediate provider may remove the authenticated caller ID information: (1) where necessary for technical reasons to complete the call; and (2) where the intermediate provider reasonably believes the caller ID authentication information presents an imminent threat to its network security. *Id.* § 64.6302(a)(1)-(2).

authenticate caller ID information for all SIP calls it receives for which the caller ID information has not been authenticated[37] or, in the alternative, cooperatively participate with the industry traceback consortium and respond fully and in a timely manner to all traceback requests regarding calls for which it acts as an intermediate provider.[38]

10. In May 2022, the Commission extended robocall mitigation and caller ID authentication obligations to gateway providers.[39] Specifically, by June 30, 2023, gateway providers must authenticate unauthenticated SIP traffic carrying a U.S. NANP number in the caller ID field,[40] and, as of January 11, 2023, must have developed and implemented robocall mitigation programs with respect to calls that are carrying a U.S. number in the caller ID field.[41] Gateway providers must also submit certifications to the Robocall Mitigation Database stating whether they have fully, partially, or not implemented STIR/SHAKEN on the IP portions of their networks[42] and describing how they are complying with the "know-your-upstream-provider" obligation,[43] which requires gateway providers to take reasonable and effective steps to ensure that the immediate upstream foreign provider is not using the gateway provider to carry or process a high volume of illegal traffic onto the U.S. network.[44]

B. Fifth Further Notice of Proposed Rulemaking

11. In May 2022, the Commission adopted the *Fifth Caller ID Authentication Further Notice*, which proposed and sought comment on extending the Commission's robocall mitigation and caller ID authentication rules to cover additional providers along the call path, as well as several additional measures to help protect American consumers from illegal robocalls.[45] First, we proposed to require all U.S. intermediate providers to use STIR/SHAKEN to authenticate caller ID information for SIP calls that are carrying a U.S. number in the caller ID field[46] and to require all voice service providers, intermediate providers, and gateway providers to comply with the most recent versions of the STIR/SHAKEN standards "adopted as of the compliance deadline" for non-gateway intermediate providers.[47]

---

[37] *Id.* § 64.6302(b).

[38] *Id.* § 64.6302(b)(1)-(2).

[39] *Gateway Provider Order* at 28, para. 59; *see also* 47 CFR § 64.6300(d) (defining "gateway provider" as a "U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider").

[40] 47 CFR § 64.6302(c); *Gateway Provider Order* at 28, para. 59.

[41] *See* 47 CFR § 64.6305(b); *Gateway Provider Order* at 15, 16, paras. 32, 34; *Wireline Competition Bureau Announces Deadlines for Gateway Provider Robocall Mitigation Requirements and Additional Compliance Dates and Filing Instructions*, WC Docket No. 17-97, Public Notice, DA 22-1303, at 2 (WCB Dec. 12, 2022). The robocall mitigation programs must include: (1) reasonable steps to avoid carrying or processing illegal robocall traffic; (2) a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium; and (3) a commitment to cooperate with such entities in investigating and stopping any illegal robocallers that use the gateway provider's service to carry or process calls. 47 CFR § 64.6305(b)(2).

[42] 47 CFR § 64.6305(d)(1).

[43] 47 CFR § 64.6305(d)(2)(ii); *id*. § 64.1200(n)(4) (know-your upstream provider requirement); *Gateway Provider Order* at 17, para. 37.

[44] 47 CFR § 64.1200(n)(4); *Gateway Provider Order* at 41, para. 96.

[45] *Fifth Caller ID Authentication Further Notice* at 63-88, paras. 157-225. The Commission also sought comment on several issues outside of the scope of this *Sixth Report and Order*. *See id.* at 68-75, 87-88, paras. 174-94, 218-23, 225.

[46] *Id.* at 63-64, 66, paras. 160, 162, 167.

[47] *Id.* at 67, para. 172.

12. Second, we sought comment on extending certain robocall mitigation duties that are currently only applicable to subsets of providers to *all* domestic providers, including: (1) extending the requirement to respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium within 24 hours of receipt of the request to all U.S.-based providers in the call path;[48] (2) requiring all domestic providers in the call path to block illegal traffic when notified of such traffic by the Commission;[49] (3) requiring providers to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls;[50] (4) requiring intermediate providers and terminating providers to block traffic from bad-actor providers when notified by the Commission, regardless of whether or not the bad actor is a gateway provider;[51] and (5) extending a general mitigation standard to all domestic intermediate providers and voice service providers that have implemented STIR/SHAKEN in the IP portions of their networks, including the duty to take "reasonable steps" to avoid originating or terminating (for voice service providers) or carrying or processing (for intermediate providers) illegal robocall traffic.[52]

13. Third, we proposed to extend robocall mitigation database filing obligations to all domestic intermediate providers regardless of their STIR/SHAKEN status.[53] Fourth, we sought comment on certain rules regarding caller ID authentication and attestation in the Robocall Mitigation Database, including whether to allow third-party authentication and whether to require all domestic providers to authenticate caller ID information using their own SPC tokens.[54] Finally, we also sought comment on several additional measures to protect American consumers against illegal robocalls, including: (1) strengthening the Commission's enforcement rules;[55] (2) clarifying aspects of the STIR/SHAKEN framework for providers lacking facilities necessary to implement STIR/SHAKEN;[56] and (3) addressing issues related to satellite voice service providers.[57]

[48] *Id.* at 69-70, paras. 177-80.

[49] *Id.* at 70, para. 181.

[50] *Id.* at 70-71, paras. 183-86.

[51] *Fifth Caller ID Authentication Further Notice* at 71-72, para. 187.

[52] *Id.* at 72-75, paras. 188-94.

[53] *Id.* at 76-79, paras. 195-200.

[54] *Id.* at 87, para. 224.

[55] *Id.* at 79-82, paras. 207-12.

[56] *Id.* at 82-83, paras. 213-15.

[57] *Fifth Caller ID Authentication Further Notice* at 83-84, paras. 216-17.

III. SIXTH REPORT AND ORDER

14. Today, we take further steps to combat illegally spoofed robocalls by expanding caller ID authentication and robocall mitigation obligations and creating new mechanisms to hold bad actors accountable for violations of our rules. Specifically, we adopt the first mandatory authentication requirement for intermediate providers to capture calls that are not authenticated by originating providers. We require *all* providers to take reasonable steps to mitigate illegal robocalls and file mitigation plans in the Robocall Mitigation Database—regardless of their STIR/SHAKEN status or whether they have the facilities necessary to implement STIR/SHAKEN. We also give the Enforcement Bureau new tools to impose penalties against bad actors, including the ability to remove the section 214 and other Commission authorizations, licenses, and certifications of repeat offenders and establish a process to expel providers that commit certain violations of our rules from the Robocall Mitigation Database on an expedited basis. Finally, we define the STIR/SHAKEN obligations of satellite providers.

A. Strengthening the Intermediate Provider Authentication Obligation

1. Requiring the First Intermediate Provider to Authenticate Unauthenticated Calls

15. Under the Commission's caller ID authentication rules, intermediate providers are required to authenticate any unauthenticated caller ID information for the SIP calls they receive or, alternatively, cooperate with the industry traceback consortium and timely and fully respond to all traceback requests received from the Commission, law enforcement, and the industry traceback consortium.[58] In the *Fourth Call Blocking Order*, however, the Commission required all providers in the path of a SIP call—including gateway providers and other intermediate providers—to respond fully and in a timely manner to traceback requests.[59] As a result of that action, intermediate providers may decline to authenticate caller ID information given that compliance with the traceback alternative has been made mandatory.[60] In the *Fifth Caller ID Authentication Further Notice*, we proposed closing this gap in the STIR/SHAKEN caller ID authentication regime by requiring all U.S. intermediate providers in the path of a SIP call carrying a U.S. number in the caller ID field to authenticate unauthenticated caller ID information, irrespective of their traceback obligations.[61] Based on our review of the record, we adopt our proposal to establish a mandatory caller ID authentication obligation for intermediate providers, but do so on an incremental basis. Specifically, we amend our rules to require any non-gateway intermediate provider that receives an unauthenticated SIP call directly from an originating provider to authenticate the call. Stated differently, the first intermediate provider in the path of an unauthenticated SIP call will now be subject to a mandatory requirement to authenticate the call.

16. The Commission has previously recognized that the STIR/SHAKEN framework has beneficial network effects and becomes more effective as more providers implement it.[62] The record in this proceeding supports expanding STIR/SHAKEN implementation by requiring non-gateway intermediate providers to authenticate unauthenticated calls, regardless of their traceback obligations.[63]

---

[58] *See* 47 CFR § 64.6302(b)(1)-(2); *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1926, para. 140. The Commission took this approach to minimize concerns about costs to intermediate providers and burdens on their networks. *See id.* at 1927-29, paras. 144-146, n.504-510.

[59] *Fourth Call Blocking Order*, 35 FCC Rcd at 15227-29, paras. 15-21; *see* 47 CFR § 64.1200(n)(1). The Commission later enhanced this obligation for gateway providers to require response within 24 hours. *Gateway Provider Order* at 30-33, paras. 65-71.

[60] *See Fifth Caller ID Authentication Further Notice* at 64, para. 162.

[61] *See Fifth Caller ID Authentication Further Notice* at 63-67, paras. 160-71.

[62] *Gateway Provider Order* at 27-28, para. 58.

[63] *See, e.g.*, Comcast Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 5 (rec. Aug. 17, 2022) (Comcast Comments); NCTA Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 2 (rec. Aug. 17, 2022) (NCTA (continued….)

As NCTA observes, "[t]he greater the number of providers that have implemented STIR/SHAKEN on their networks, the harder it will be for malicious callers to evade call authentication and harm consumers."[64] Similarly, Comcast notes that "the benefits of STIR/SHAKEN will multiply as implementation becomes more widespread."[65] Although originating providers are required to authenticate calls under the Commission's rules—with limited exceptions—some originating providers are not capable of implementing STIR/SHAKEN.[66] In other cases, unscrupulous providers may deliberately fail to comply with our rules.[67] The record shows that the failure of originating providers to sign calls is one of the key weaknesses in the STIR/SHAKEN regime.[68] By requiring intermediate providers to authenticate unauthenticated SIP calls they receive directly from an originating provider, we close an important loophole in our caller ID authentication scheme, and incorporate calls that would otherwise go unauthenticated into the STIR/SHAKEN framework. Further, intermediate provider authentication will facilitate analytics, blocking, and traceback efforts by providing more information to downstream providers.[69]

17. We recognize, however, that a mandatory authentication obligation could subject intermediate providers to significant costs.[70] For example, Verizon argues that "[a]n intermediate

(Continued from previous page)
Comments); INCOMPAS Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 6-7 (rec. Aug. 17, 2022) (INCOMPAS Comments).

[64] NCTA Comments at 2 (encouraging the Commission to "bring all U.S. providers within the STIR/SHAKEN regime by adopting its proposal to require that intermediate providers authenticate unauthenticated calls they receive").

[65] Comcast Comments at 3-5 (supporting widespread adoption of the STIR/SHAKEN authentication framework and stating that "the time is now ripe," for the Commission to require "all U.S. intermediate providers to authenticate unsigned calls they receive using STIR/SHAKEN before passing them along to another provider").

[66] *See* 47 CFR § 64.6304(a)(1)(i) (providing an extension of the implementation deadline for non-facilities based small voice service providers until June 30, 2022); *id.* § 64.6304(b) (SPC token access exception).

[67] YouMail Comments, CG Docket No. 17-59 at 12 (Aug. 16, 2022) (YouMail Comments) ("While most originating providers are actively working to identify and stop sources of robocalls, others are factually or implicitly 'partners' with fraudsters, failing to take needed actions to stop robocalls."); Fifty-One State Attorneys General Reply, CG Docket No. 17-59, WC Docket No. 17-97, CG Docket No. 17-59, WC Docket No. 17-97, at 3 (State AGs Reply); ZipDX Reply, CG Docket No. 17-59, WC Docket No. 17-97, at 5-6 (rec. Sept. 19, 2022) (ZipDX Reply).

[68] USTelecom Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 10 (rec. Aug. 17, 2022) (USTelecom Comments) (arguing that bad-actor originating providers "do not sign their calls" and attempt to evade detection by relying on downstream providers to authenticate illegal traffic with the downstream provider's token, thereby "undermin[ing] the accountability the STIR/SHAKEN framework is intended to impose"); ZipDX Reply at 5-6 ("[T]he biggest Call Authentication issue with robocalls . . . is that they are not being signed by the originating provider despite existing rules.").

[69] *See* North American Numbering Council, Call Authentication Trust Anchor Working Group, Best Practices for Terminating Voice Service Providers using Caller ID Authentication Information § 2.1.2 at 7 (Feb. 9, 2022), https://nanc-chair.org/docs/CATA_Report_Best_Practices_for_Terminating_VSPs_using_Caller_ID_Authentication_Information_Feb_2022.pdf (noting that information sent along with the authentication allows the traceback process to quickly identify who signed the call, regardless of the attestation level) (2022 NANC Best Practices for Terminating Voice Service Providers); *Fifth Caller ID Authentication Report and Order* at 25-27, para. 57; Comcast Comments at 5-6; INCOMPAS Comments at 6; *see also* Telnyx Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 1 (rec. Aug. 17, 2022) (Telnyx Comments) (acknowledging that intermediate provider authentication will "expedit[e] the traceback process," but arguing that such a requirement "might do more harm than good").

[70] USTelecom Comments at 11-12; USTelecom Reply, CG Docket No. 17-59, WC Docket No. 17-97, at 3, 14 (rec. Sept. 16, 2022) (USTelecom Reply); Verizon Reply, CG Docket No. 17-59, WC Docket No. 17-97, at 6-9 (rec. Sept. 16, 2022) (Verizon Reply).

provider attestation mandate would involve substantial carrier work streams and vendor development costs," and cause technical challenges for terminating providers.[71] USTelecom argues that, while intermediate providers "have ensured that their networks can pass along STIR/SHAKEN information they receive, it is an entirely different—and expansive and costly—effort to ensure that each and every switch can sign calls."[72] We therefore opt to take an incremental approach to imposing mandatory authentication obligations on intermediate providers, requiring only the first intermediate provider in the path of a SIP call to authenticate unauthenticated caller ID information, rather than requiring all intermediate providers in the path to do so at this time.[73] We find that this approach, which focuses on the beginning of the call path, will directly address the problem of calls entering the call path without being authenticated by originating providers, as described above. We agree with YouMail that this targeted approach is likely to have the greatest impact on stopping illegally spoofed robocalls.[74] While the Commission may consider expanding a call authentication requirement to all intermediate providers in the future, this targeted approach will provide the Commission with an opportunity to evaluate this first mandatory obligation for

[71] Verizon Reply at 7-9.

[72] USTelecom Comments at 11. Some commenters also argue that requiring all non-gateway intermediate providers to authenticate unauthenticated SIP calls could result in calls that were given an A-level attestation by originating providers being later given a C-level attestation if the call traverses a non-IP network, and that this increase in C-level attestations could impede efforts by downstream providers, analytics vendors, and others to accurately identify illegal robocalls in some situations. *See, e.g.*, INCOMPAS Comments at 8; Telnyx Comments at 2; USTelecom Comments at 11; Verizon Reply at 6-8. While we generally agree that higher-level attestations are more advantageous than C-level attestations, as we stated in the *Gateway Provider Order*, where a call is unauthenticated, a C-level attestation is better than no attestation and has value. *Gateway Provider Order* at 25-27, para. 57. Nevertheless, for the reasons stated herein, we believe that the goals of the STIR/SHAKEN framework and the public interest are best served by taking a targeted approach to intermediate provider authentication that focuses on the first intermediate provider in the call path.

[73] Intermediate providers should know whether they receive calls directly from an originating provider pursuant to contracts that provide information to the intermediate provider about the originating provider's customers and expectations for handling their traffic. *See Rural Call Completion*, WC Docket No. 13-39, Fourth Report and Order, 34 FCC Rcd 1781, 1786, para. 24 (2019) (noting that intermediate providers maintain contractual relationships with the upstream providers from which they receive traffic and imposing requirements based on those contractual relationships). Further, as explained in Section III.B below, we require non-gateway intermediate providers to take "reasonable steps" to mitigate illegal robocall traffic. That duty, along with other requirements of our rules, may require intermediate providers to perform the due diligence necessary to understand the sources of the traffic it receives. *See* 47 CFR § 64.6305(e). Accordingly, in the unlikely event that an intermediate provider does not know through its contracts whether it receives calls directly from an originating provider, it should obtain that information to comply with this and other aspects of the Commission's rules. *See* Cloud Communications Alliance Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 9 (rec. Aug. 17, 2022) (CCA Comments) (writing in favor of expanding robocall mitigation requirements and noting that "[a]ll providers should take basic, reasonable steps to vet their customers, whether the customer is a business end user or another provider, before initiating service"); USTelecom Comments at 8-9 (advocating for the Commission to expand robocall mitigation requirements to all providers and writing that for intermediate providers, "robocall mitigation efforts should include at least a basic level of vetting of the providers immediately upstream from whom they accept traffic"); Verizon Reply at 5 (suggesting that the Commission should encourage the industry to "undertake [know your customer] evaluations of upstream service providers and to create an end-to-end 'chain of trust' between good callers and terminating service providers").

[74] *See* YouMail Comments at 10 ("In determining which rules should apply to which service providers, [the Commission] should focus on the effect those providers can have on minimizing the number of robocalls received by consumers."). As YouMail argues, apart from the originating provider, the "best entity to identify and stop the sources of robocalls is the first 'downstream' provider (*i.e.*, the next provider in line that receives calls placed on the originating provider's network)." *Id*. at 13.

intermediate providers, together with other pending expansions of the caller ID authentication regime,[75] and determine whether an authentication requirement for more downstream intermediate providers is warranted.[76]

18. We are not persuaded by the arguments submitted by commenters favoring a mandatory authentication requirement for all intermediate providers. For instance, some commenters argue that the Commission's justifications for adopting a mandatory gateway provider authentication requirement apply with equal force to all non-gateway intermediate providers in the call path.[77] We disagree. The gateway provider caller ID authentication rules adopted by the Commission in May 2022 apply to the first domestic intermediate provider in the path of a foreign-originated call.[78] The authentication requirement we adopt today similarly applies to the first intermediate provider in the path of a U.S.-originated call. Further, there are fewer gateway providers than other domestic intermediate providers.[79] Therefore, the overall industry cost of an authentication obligation imposed on all domestic intermediate providers is likely to be significantly higher than that of the gateway provider obligation.[80] The record in this proceeding simply does not support requiring all intermediate providers to incur those costs at this time if imposing an authentication obligation on the first intermediate provider that receives an unauthenticated call directly from an originating provider can close significant gaps in our caller ID authentication regime.[81] We find that the incremental approach we adopt today will target a critical gap in our call

[75] *See Gateway Provider Order* at 22-28, paras. 51-63; 47 CFR § 64.6302(c) (requiring gateway providers to implement STIR/SHAKEN to authenticate SIP calls that are carrying a U.S. number in the caller ID field by June 30, 2023); *Second Reevaluation of STIR/SHAKEN Extensions Public Notice* at 1 (noting that "[t]he extension for facilities-based small voice service providers will lapse on June 30, 2023, marking a significant step toward the Commission's goal of achieving ubiquitous STIR/SHAKEN implementation").

[76] *See* RingCentral Comments at 2 (supporting the Commissions "recent actions to broaden the scope of providers and traffic subject to call authentication requirements" but cautioning that some of these requirements are not yet in effect and that "more time is needed to determine the efficacy of these measures" before adopting "sweeping new measures"); YouMail Comments at 13-14 (arguing that "imposing additional requirements on the first downstream provider is reasonable and an efficient area for FCC action"); *see also* CCA Comments at 3 (arguing that "it may be prudent to take a pause" prior to "adopting further rules or extending existing obligations"); INCOMPAS Comments at 4 (urging the Commission "not to create, extend, or clarify obligations without conducting a thorough assessment of the impact its existing requirements are having on illegal robocalls and providers").

[77] *See* Comcast Comments at 5 ("The Commission notably just imposed this very obligation on gateway providers, and the same justifications cited in that context support extending this obligation to all U.S. intermediate providers."); State AGs Reply at 5.

[78] *See Gateway Provider Order* at 12, 22-24, paras. 25, 51-54 (defining the term "gateway provider" and explaining the scope of the authentication requirement for such providers).

[79] There are currently 129 gateway provider filings (including combined gateway provider/voice service provider filings) and 1,137 non-gateway intermediate provider filings (including filings imported from the Intermediate Provider Registry) in the Robocall Mitigation Database. FCC, Robocall Mitigation Database, https://fccprod.servicenowservices.com/rmd?id=rmd_listings (last visited Feb. 16, 2023).

[80] As noted above, we only apply this requirement to the first downstream intermediate provider in a given call path. Therefore, downstream intermediate providers that carry the call throughout the rest of a given call path will not face compliance costs related to this rule. Per our existing rules, however, any intermediate provider is still required to pass unaltered the authenticated caller identification information it receives for a SIP call to the subsequent intermediate or voice service provider in the call path, subject to limited exceptions. 47 CFR § 64.6302; *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1922-1929, paras. 133-39, 148.

[81] *See* RingCentral Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 1, 6 (rec. Aug. 17, 2022) (RingCentral Comments) (arguing that "[s]weeping requirements that are not targeted specifically at illegal traffic will . . . impose heavy burdens on service providers, and harm competition and market entry," and that the Commission should consider the impact of new requirements on new entrants to the market, including small and women-and minority-owned businesses).

authentication regime while minimizing the impact of our requirements on industry, including new entrants to the market.

19. We also decline to impose an authentication obligation on all intermediate providers at this time to address instances in which authentication information is "stripped out" by the call transiting a non-IP network.[82] The Commission has launched an inquiry into solutions to enable caller ID authentication over non-IP networks, the nexus between non-IP caller ID authentication and the IP transition generally, and on specific steps the Commission can take to encourage the industry's transition to IP.[83] Widespread adoption of a non-IP authentication solution or IP interconnection would result in authenticated caller ID information being preserved and received by the terminating provider.[84] We therefore decline to impose an authentication obligation on all intermediate providers to address circumstances where a call traverses a non-IP network, but may revisit the subject after the Commission concludes its inquiry into whether non-IP authentication or IP interconnection solutions are feasible and can be timely implemented.

20. Finally, we note that the requirement we adopt here for the first intermediate provider to authenticate a call will arise in limited circumstances, such as where the originating provider failed to comply with their own authentication obligation or where the call is sent directly to an intermediate provider from the limited subset of originating providers that lack an authentication obligation.[85] Indeed, the first intermediate provider in the call path may completely avoid the need to authenticate calls if it implements contractual provisions with its upstream originating providers stating that it will only accept authenticated traffic.

2. Applicable STIR/SHAKEN Standards for Compliance

21. Voice service providers and gateway providers are obligated to comply with, *at a minimum*, the version of the STIR/SHAKEN standards ATIS-1000074, ATIS-1000080, and ATIS-1000084 and all of the documents referenced therein in effect at the time of their respective compliance deadlines, including any errata as of those dates or earlier.[86] In the *Fifth Caller ID Authentication Further Notice*, we proposed that non-gateway intermediate providers comply with, at a minimum, the versions of these standards in effect at the time of their compliance deadline.[87] We also sought comment on whether all providers should be required to comply with the same versions of the standards as non-gateway intermediate providers and whether we should establish a mechanism for updating the standard that

[82] *See* State AGs Reply at 4 (arguing that the Commission should require "all intermediate providers to comply with STIR/SHAKEN so that they no longer strip" information required by STIR/SHAKEN authentication protocols from calls); ZipDX Reply at 5. As noted above, our rules already require intermediate providers to "[p]ass unaltered to the subsequent intermediate provider or voice service provider in the call path any authenticated caller identification information it receives with a SIP call," subject to limited exceptions. 47 CFR § 64.6302.

[83] *See generally Non-IP Authentication Notice of Inquiry*.

[84] *See Non-IP Authentication Notice of Inquiry* at 4, 17-18, paras. 6, 37; INCOMPAS Comments at 8 (while supporting intermediate authentication, arguing that IP interconnection would solve the same problem without "flooding the ecosystem with 'B' or 'C' level calls"); Telnyx Comments at 2 (arguing the Commission should focus on the promotion of IP interconnection instead of intermediate provider authentication).

[85] If the originating provider complies with its authentication obligation, the first intermediate provider in the call chain need only meet its preexisting obligation to pass-on that authentication information to the next provider in the chain. 47 CFR §§ 64.6301(a)(2); 64.6302(a). There are two exceptions to this rule under which an intermediate provider may remove the authenticated caller ID information: (1) where necessary for technical reasons to complete the call; and (2) where the intermediate provider reasonably believes the caller ID authentication information presents an imminent threat to its network security. *See* 47 CFR § 64.6302(a)(1)-(2).

[86] *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3258-59, para. 36; *see also Gateway Provider Report and Order* at 23-24, para. 53.

[87] *Fifth Caller ID Authentication Further Notice* at 66, para. 168.

providers must comply with going forward, including through delegation to the Wireline Competition Bureau.[88]

22. We adopt our proposal that non-gateway intermediate providers subject to the authentication obligation described above must comply with, at a minimum, the versions of the standards in effect at the time of their authentication compliance deadline (which is addressed in the following section), along with any errata. Like other providers, non-gateway intermediate providers will have the "flexibility to assign the level of attestation appropriate to the call based on the applicable level of the standards and the available call information."[89] This approach is supported in the record.[90]

23. We do not at this time require gateway and voice service providers to comply with versions of the standards that came into effect after their respective compliance deadlines. As USTelecom notes, the implementation costs of a new version of the standards may outweigh its benefits, particularly for providers that have already spent time and expense implementing an older version of the standard and where the new standard may provide only marginal benefits.[91] We reiterate, however, that our requirement that providers must comply with a specific version of a standard "at a minimum," means that while providers are required to comply with these standards, they are *permitted* to comply with any version of the standard that has been ratified by ATIS subsequent to the standard in effect at the time their authentication implementation deadline.[92]

24. We nevertheless conclude that there may be significant benefits for all providers to comply with standards as they are updated, particularly where updated versions contain critical new features or functions. Requiring all providers to comply with a single, updated standard would also facilitate enforcement of our rules and ensure that any new features and functions contained in revised standards spread throughout the STIR/SHAKEN ecosystem. Therefore, we adopt a process to incorporate future standards into our rules where appropriate, similar to the process we have adopted to require compliance with updated technical standards in other contexts.[93]

25. Specifically, we delegate to the Wireline Competition Bureau the authority to determine whether to seek comment on requiring compliance with revised versions of the three ATIS standards associated with the STIR/SHAKEN authentication framework, and all documents referenced therein. We also delegate to the Wireline Competition Bureau the authority to require providers subject to a

[88] *Id.* at 67, para. 172.

[89] *Id.* para. 171 (proposing a flexible approach for all intermediate providers consistent with the rules applicable to voice service providers and gateway providers); *see also id.* at 24, para. 54 (adopting rule for gateway providers); *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1926-27, paras. 142-43 (adopting rule for voice service providers).

[90] *See e.g.*, Comcast Comments at 6; NCTA Comments at 2 n.3.

[91] USTelecom Comments at 13 & n.32.

[92] *First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3258-59, para. 36 (noting that the ATIS standards were designed to evolve and improve over time and stating that the Commission, "intend[ed] for [the Commission's] rules to provide this same room for innovation, while maintaining an effective caller ID authentication ecosystem."). However, any later-adopted or improved version of the standards that a provider chooses to incorporate into its STIR/SHAKEN authentication framework must maintain the baseline call authentication functionality exemplified by the versions of ATIS-1000074, ATIS-1000080, and ATIS-1000084 in effect at the time of its respective compliance date. *Id*.

[93] *See, e.g.*, 47 CFR § 20.19(k)(1) (delegating authority for adoption of ANSI C63 standards for wireless handset hearing-aid-compatibility "provided that the standards do not impose with respect to such frequency bands or air interfaces materially greater obligations than those impose on other services subject to this section"); *id*. § 52.26(b)(4) (providing process for adopting the North American Numbering Council number portability recommendations).

STIR/SHAKEN authentication requirement to comply with those revised standards, and the authority to set appropriate compliance deadlines regarding such revised standards.[94] Providers will only be required to implement new standards if the benefits to the STIR/SHAKEN ecosystem outweigh any compliance burdens. Additionally, a process based on delegated authority may allow the adoption of revised standards more quickly than would be the case through Commission-level notice and comment procedures.

26. As with voice service and gateway providers, we also require any non-gateway intermediate provider subject to the authentication obligation described in this section to either upgrade its network to allow for the initiation, maintenance, and termination of SIP calls and fully implement the STIR/SHAKEN framework, or "[m]aintain and be ready to provide the Commission on request with documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non-internet Protocol caller identification authentication solution, or actively testing such a solution."[95] We find that expanding the requirements of section 64.6303 to non-gateway intermediate providers will ensure regulatory parity and promote the development of non-IP authentication solutions, while offering flexibility to providers that rely on non-IP infrastructure.

3. Compliance Deadlines

27. We set a December 31, 2023 deadline for the new authentication obligations adopted in this section. By that date, the first non-gateway intermediate provider in the call chain must authenticate unauthenticated calls it receives. We adopt a deadline longer than the six-month deadline we suggested in the *Fifth Caller ID Authentication Further Notice* because intermediate providers need time to deploy the technical capability to comply with our requirement to authenticate calls, and providers may wish to amend their contracts with upstream originating providers to meet this new requirement.[96] While the record reflects disagreement as to an appropriate intermediate authentication provider deadline,[97] we conclude that a later deadline is not necessary. Implementation of call authentication technology has likely become faster and less costly for many providers than when the Commission first adopted caller ID authentication requirements, particularly for those that have already implemented STIR/SHAKEN in their other roles in the call stream.[98] Moreover, a non-gateway intermediate provider can avoid the need to

[94] *See Fifth Caller ID Authentication Further Notice* at 67, para. 172.

[95] 47 CFR § 64.6303. In the *Fifth Caller ID Authentication Further Notice*, we sought comment on whether to "require all providers to adopt a non-IP caller ID authentication solution," and noted that under the Commission's rules "[v]oice service providers and gateway providers currently have a choice whether to implement a non-IP caller ID authentication solution or, in the alternative, participate with a working group, standards group, or consortium to develop a solution." *Fifth Caller ID Authentication Further Notice* at 67-68, para. 173 (citing 47 CFR § 64.6303).

[96] The *Fifth Caller ID Authentication Further Notice* sought comment on, but did not propose, a specific compliance deadline. *See Fifth Caller ID Authentication Further Notice* at 67, para. 169 (seeking comment on whether we should "require all intermediate providers to authenticate all unauthenticated SIP calls carrying U.S. NANP numbers within six months after we adopt an order released pursuant to this Further Notice").

[97] *See* Comcast Comments at 6 (arguing for a deadline no sooner than June 30, 2023); INCOMPAS Comments at 8 (arguing for a 12-month deadline to "more closely match the deadlines offered to other voice providers that have been required to adopt the STIR/SHAKEN framework"); State AGs Reply at 5 (arguing for action "as soon as possible").

[98] *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Fourth Further Notice of Proposed Rulemaking, 36 FCC Rcd 14971, 14988, para. 42 (*Gateway Provider Further Notice*); *see also Gateway Provider Order* at 24, para. 56 (noting that gateway providers' authentication costs will be limited for those providers that have implemented authentication as voice service providers); ZipDX Comments at 5-6 (noting that "many intermediates also serve as originating providers and so have been subject to authentication requirements in that role").

implement STIR/SHAKEN where it agrees to only accept authenticated traffic from originating providers.[99]

B. Mitigation and Robocall Mitigation Database Filing Obligations

28. We next take action to strengthen the robocall mitigation requirements and Robocall Mitigation Database filing obligations of all providers. As we proposed in the *Fifth Caller ID Authentication Further Notice*, we require *all* providers—including intermediate providers and voice service providers without the facilities necessary to implement STIR/SHAKEN—to: (1) take "reasonable steps" to mitigate illegal robocall traffic; (2) submit a certification to the Robocall Mitigation Database regarding their STIR/SHAKEN implementation status along with other identifying information; and (3) submit a robocall mitigation plan to the Robocall Mitigation Database.[100] Consistent with our proposal, we also require downstream providers to block traffic received directly from all intermediate providers that are not in the Robocall Mitigation Database.[101] These actions have significant support in the record.[102] While we do not require providers to take specific steps to meet their mitigation obligations, we do expand the subjects that providers must describe in their filed mitigation plans and the information that providers must submit to the Robocall Mitigation Database.

1. Applying the "Reasonable Steps" Mitigation Standard to All Providers

29. We adopt our proposal in the *Fifth Caller ID Authentication Further Notice* to expand to all providers the obligation to mitigate illegal robocalls under the general "reasonable steps" standard.[103] Specifically, we now require all non-gateway intermediate providers, as well as voice service providers that have fully implemented STIR/SHAKEN, to meet the same "reasonable steps" general mitigation standard that is currently applied to gateway providers and voice service providers that have not fully implemented STIR/SHAKEN under the Commission's rules.[104] We also conclude that voice service providers without the facilities necessary to implement STIR/SHAKEN must mitigate illegal robocalls and meet this same mitigation standard.[105]

---

[99] The Commission has previously found that six months is sufficient time for providers to evaluate and renegotiate contracts to address new regulatory requirements. *See Rural Call Completion*, WC Docket No. 13-39, Second Report and Order, 33 FCC Rcd 4199, 4222, para. 50 (2018) (finding that a six-month transition period would provide sufficient time for providers to "evaluate and renegotiate contracts with intermediate providers" in order to comply with the rural call completion monitoring rule). Accordingly, we find that the approximate nine-month period afforded by the December 31, 2023 deadline provides sufficient time for intermediate providers to amend their contracts with originating providers, if necessary, to comply with our authentication requirement.

[100] *See Fifth Caller ID Authentication Further Notice* at 72-73, 75, paras. 188, 195.

[101] *Id.* at 79, para. 205.

[102] We discuss the record support in response to the *Fifth Caller ID Authentication Further Notice* below. There was also significant support for taking some of these actions in response to the *Gateway Provider Further Notice*, but we did not act at that time given the limited scope of that proceeding. *Gateway Provider Order* at 19, paras. 42-43; *see also* CTIA *Gateway Provider Further Notice* Comments at 7; iBasis *Gateway Provider Further Notice* Comments at 13; Twilio *Gateway Provider Further Notice* Comments at 3; USTelecom *Gateway Provider Further Notice* Comments at 4-7; ZipDX *Gateway Provider Further Notice* Comments at 32-33.

[103] *Fifth Caller ID Authentication Further Notice* at 72, para. 188.

[104] 47 CFR § 64.6305(a)(2), (b)(2); *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1899, para. 76 (for voice service providers); *Gateway Provider Order* at 43, para. 102 (for gateway providers). The general mitigation standard we adopt here for all providers is separate from and in addition to the new robocall mitigation program description obligations for all providers discussed below. *See infra* Section III.B.2; *cf.* 47 CFR § 64.6305(c)(2) (robocall mitigation program description requirement for voice service providers), (d)(2) (robocall mitigation program description requirement for voice service providers).

[105] *Fifth Caller ID Authentication Further Notice* at 82, para. 214 (seeking comment on requiring these providers to perform robocall mitigation).

30. Requiring all providers to mitigate calls under the "reasonable steps" standard will ensure that every provider in the call chain is subject to the same duty to mitigate illegal robocalls, promoting regulatory symmetry and administrability.[106] There is significant support in the record for this approach.[107] For providers with a STIR/SHAKEN authentication obligation, these mitigation duties will serve as an "effective backstop" to that authentication obligation and, for those without such an obligation, they will act as a key bulwark against illegal robocalls.[108] As the Commission has noted, STIR/SHAKEN is not a silver bullet[109] and has a limited effect on illegal robocalls where the number was obtained lawfully and not spoofed.[110] Requiring all providers to take reasonable steps to mitigate illegal robocalls will help address these limitations in the STIR/SHAKEN regime.[111]

31. As proposed,[112] we retain a general standard that requires providers to take "reasonable steps" to mitigate illegal robocall traffic,[113] rather than mandate that providers include specific measures as part of their mitigation plans.[114] Pursuant to this standard, a provider's program is "sufficient if it includes detailed practices that can reasonably be expected to significantly reduce" the carrying or

[106] Comcast Comments at 10-11; State AGs Reply at 10-11 (arguing that extending mitigation requirements "to all domestic providers will also simplify rules for all stakeholders . . . subjecting them to the same obligations for all calls, regardless of the providers' respective roles in the call path").

[107] *See, e.g.*, CCA Comments at 5; Comcast Comments at 10-11 (supporting imposing mitigation and mitigation plan filing obligations on voice service providers that have implemented STIR/SHAKEN and intermediate providers); INCOMPAS Comments at 14-15 (supporting applying general mitigation standard to all providers, but without prescribing specific steps); NCTA Comments at 3-4; New York State Public Service Commission (NYPSC) Comments at 1-2; USTelecom Comments at 8; Voice On The Net Coalition (VON) Comments at 4; State AGs Reply at 4; TransNexus Reply at 12.

[108] *See Fifth Caller ID Authentication Further Notice* at 72, para. 188; INCOMPAS Comments at 16-17 ("INCOMPAS believes providers that are otherwise unable to implement STIR/SHAKEN should be required to conduct some essential robocall mitigation tasks that will protect consumers from illegal robocalls.").

[109] *Gateway Provider Order* at 44, para. 105; State AGs Reply at 4; *see also* Comcast Comments at 4 (noting that "STIR/SHAKEN is not a panacea"); USTelecom Reply at 2 (noting that "there is no magic bullet solution that will once and for all solve the illegal robocall problem").

[110] *See Gateway Provider Order* at 44, para. 105; USTelecom Comments at 8 ("STIR/SHAKEN alone will not prevent bad actors from making illegal robocalls because, while it provides important information about whether the calling number can be trusted, STIR/SHAKEN does not address whether a given call is legal or illegal. Indeed, robocallers already have responded by making bad calls with numbers they obtain lawfully. Merely signing calls is not enough, because a bad call from a bad actor could still be signed.").

[111] We explain our authority for imposing these obligations below. *See infra* Section III.G.

[112] *Fifth Caller ID Authentication Further Notice* at 72-73, para. 188.

[113] We note, however, that what constitutes a "reasonable step" may depend upon the specific circumstances and the provider's role in the call path. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1900, para. 78 ("[W]e agree with Verizon that 'different types of network providers should have different types of robocall mitigation programs,' and we welcome voice service providers adopting approaches that are innovative, varied, and adapted to their networks." (footnote omitted)).

[114] While some commenters argue that we should require providers to take specific measures under the "reasonable steps" standard, *see* CCA Comments at 8-9; Electronic Privacy Information Center and National Consumer Law Center (EPIC/NCLC) Comments at 12 (arguing that if a "robocall mitigation plan truly consists of 'reasonable steps,' those steps should include call analytics and possibly also content analytics to identify and stop illegal calls in their tracks"); TransNexus Reply at 13, we agree that providers should retain "the necessary flexibility in determining which measures to use to mitigate illegal calls on their networks." INCOMPAS Comments at 15; *see also* Telnyx Comments at 2 (opposing "prescribed robocalling mitigation requirements due to industry and end-customer diversity"); *id*. at 3 ("[m]andating certain mitigation methods may also allow bad actors to evolve their tactics to evade" such methods).

processing (for intermediate providers) or origination (for voice service providers) of illegal robocalls.[115] Each provider "must comply with the practices" that its program requires,[116] and its program is insufficient if the provider "knowingly or through negligence" carries or processes calls (for intermediate providers) or originates (for voice service providers) unlawful robocall campaigns.[117] Providers' programs must also commit to respond fully, within the time period required by our rules,[118] to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers that use its service to originate, carry, or process illegal robocalls.[119]

32. We decline to adopt EPIC/NCLC's proposal to replace the "reasonable steps" general mitigation standard with the "affirmative, effective measures" standard found elsewhere in our rules.[120] Under EPIC/NCLC's proposal, a provider would fail to meet this standard if they allow the origination of any illegal robocalls, even where the provider may have taken "reasonable steps" to mitigate such calls.[121] We disagree with EPIC/NCLC's reading of our rules and conclude that these standards work hand-in-hand to prevent illegal robocalls. A key purpose of the "reasonable steps" standard is to ensure that providers enact a robocall mitigation program and describe that program in the Robocall Mitigation Database. If the program is not reasonable as described, or if it is not followed, the provider may be held liable.[122] Further, if the steps described in a mitigation program are followed but are not actually effective in stopping illegal robocalls, the originating provider could be held liable for failing to put in place "affirmative, effective" measures to stop robocalls if they do not take further action.[123] Regardless of the mitigation standard we adopt, we disagree with EPIC/NCLC that providers should be held strictly liable for allowing the origination of any illegal robocalls regardless of whether they have taken "reasonable steps" to mitigate such calls, as explained in more detail below.[124]

---

[115] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1900, para. 78 (obligation for voice service providers); *Gateway Provider Order* at 43-44, para. 103 (obligation for gateway providers).

[116] *Id*.

[117] *Id*. We decline to adopt VON's proposal for a safe harbor from contract breach for providers invoking contract termination provisions against providers originating illegal robocall traffic. VON Comments at 6. VON does not explain why such a safe harbor is necessary or the legal authority for the Commission to adopt such a provision, and we find it outside the scope of this proceeding.

[118] 47 CFR § 64.6305(a)(2) (requiring any robocall mitigation program for voice service providers to include a commitment to respond fully in a timely manner); *id.* § 64.6305(b)(2) (requiring any robocall mitigation program for gateway providers to include a commitment to respond fully within 24 hours).

[119] *Id.* § 64.6305(a)(2) (requirement for voice service provider robocall mitigation programs); *id.* § 64.6305(b)(2) (requirement for gateway provider robocall mitigation programs).

[120] EPIC/NCLC Comments at 8-10; *see* 47 CFR § 64.1200(n)(3); *Fourth Call Blocking Order*, 35 FCC Rcd at 15232-33, paras. 32-36 (adopting requirement that voice service providers adopt affirmative, effective measures to prevent new and renewing customers from using their network to originate illegal calls). EPIC/NCLC argues that "where providers have a responsibility to take reasonable steps to detect and mitigate illegal call traffic," its proposed "should have known" liability rule would require them to monitor call traffic. EPIC/NCLC Comments at 12.

[121] EPIC/NCLC Comments at 10-11.

[122] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1900, para. 77.

[123] 47 CFR § 64.1200(n)(3). Similarly, the provider may also be liable if its program "knowingly or through negligence" allows the origination, carrying, or processing of illegal robocalls. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1900, para. 78 (obligation for voice service providers); *Gateway Provider Order* at 44, para. 103 (obligation for gateway providers).

[124] *See infra* Section III.C.5.

33. We also do not adopt VON's proposal of a "gross negligence" standard to evaluate whether a mitigation program is sufficient,[125] rather than the Commission's existing standard, which assesses whether a provider "knowingly or through negligence" originates, carries, or processes illegal robocalls.[126] We disagree that our existing standard "essentially impose[s] strict liability on providers," as VON asserts.[127] On the contrary, if a provider is taking sufficient "reasonable steps" to mitigate illegal robocall traffic pursuant to a robocall mitigation program that complies with the Commission's rules, the provider is likely not acting negligently.

34. Lastly, we decline to adopt a heightened mitigation obligation solely for VoIP providers.[128] We acknowledge that there is evidence that VoIP providers are disproportionally involved in the facilitation of illegal robocalls.[129] However, we agree with commenters opposing such a heightened standard, because "[t]he threat of illegal robocalls is an industry issue and impacts every type of provider."[130] We find that applying our obligations to providers regardless of the technology used to transmit calls better aligns with the competitive neutrality of the TRACED Act.[131]

35. *Deadlines*. Consistent with the obligation placed on other providers and the limited comments filed in the record, we require providers newly covered by the general mitigation standard to meet that standard within 60 days following Federal Register publication of this Report and Order.[132]

2. Expanded Robocall Mitigation Database Filing Obligations

36. We next take steps to strengthen our Robocall Mitigation Database filing obligations to increase transparency and ensure that all providers act to mitigate illegal robocalls. The Commission previously required voice service providers with a STIR/SHAKEN implementation obligation[133] and

[125] VON Comments at 4.

[126] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1900, para. 78 (standard for voice service providers); *Gateway Provider Order* at 44, para. 103 (standard for gateway providers).

[127] VON Comments at 4. We discuss EPIC/NCLC's strict liability proposal more generally below. *See infra* para. 75.

[128] *See Fifth Caller ID Authentication Further Notice* at 74, para. 192 (seeking comment on whether there should be a higher burden for VoIP providers to meet the "reasonable steps" standard).

[129] *See* EPIC/NCLC Comments at 18; State AGs Reply at 3-4 (stating that "[i]llegal robocallers depend upon a relatively small number of unscrupulous VoIP providers who integrate their call traffic into the larger body of legitimate call traffic").

[130] INCOMPAS Comments at 15; *see also* Telnyx Comments at 3; VON Comments at 5. Transaction Network Services (TNS) notes that while VoIP providers are the greatest source of "high-risk calls," the distribution of such calls among VoIP providers "decreased slightly" in the first half of 2022. TNS, 2022 Robocall Investigation Report Ninth Ed. at 19 (Oct. 2022) (stating that inconsistent attestation practices make attestation data "less reliable as an analytical input") (TNS October Robocall Report).

[131] TRACED ACT § 4(a)(2) (defining voice service as "any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end user using resources from the North American Numbering Plan or any successor").

[132] *See Fifth Caller ID Authentication Further Notice* at 74-75, para. 194 (seeking comment on compliance deadline for the proposed extension of robocall mitigation program requirements to additional providers and specifically asking if a deadline "30 or 60 days after the effective date of any order" would be sufficient); INCOMPAS Comments at 15 ("If the Commission adopts an extension to the General Mitigation Standard, the agency should provide 60 days for providers to comply."). No commenter argued that a greater length of time is needed to comply, and we find no reason to depart from the same compliance timeframe previously established for other providers.

[133] By "STIR/SHAKEN implementation obligation," we mean the applicable requirement under the Commission's rules that a provider implement STIR/SHAKEN in the IP portions of their networks by a date certain, subject to certain exceptions. *See* 47 CFR § 64.6301 (implementation requirement for voice service providers); *id.* § 64.6302 (implementation requirement for intermediate providers, including gateway providers); *supra* para. 4. When

(continued….)

those subject to an extension to file certifications in the Robocall Mitigation Database regarding their efforts to mitigate illegal robocalls on their networks—specifically, whether their traffic is either "signed with STIR/SHAKEN or . . . subject to a robocall mitigation program."[134] Those voice service providers that certified that some or all of their traffic is "subject to a robocall mitigation program" were required to submit a robocall mitigation plan detailing the specific "reasonable steps" that they have taken "to avoid originating illegal robocall traffic."[135] The Commission did not specifically require voice service providers without the facilities necessary to implement STIR/SHAKEN to file certifications in the database and had previously concluded that they were "not subject to [the Commission's] implementation requirements."[136]

37. We adopt our proposal to expand the obligation to file a robocall mitigation plan along with a certification in the Robocall Mitigation Database to all providers regardless of whether they are required to implement STIR/SHAKEN—including non-gateway intermediate providers and providers without the facilities necessary to implement STIR/SHAKEN[137]—and expand the downstream blocking duty to providers receiving traffic directly from non-gateway intermediate providers not in the Robocall Mitigation Database.[138] As proposed, providers with a new Robocall Mitigation Database filing obligation must submit the same basic information as providers that had previously been required to file.[139] We also require all providers to file additional information in certain circumstances, as explained below.[140]

38. *Universal Robocall Mitigation Database Filing Obligation*. There was overwhelming record support for broadening the Robocall Mitigation Database certification and mitigation plan filing obligation to cover all providers.[141] ACA Connects notes that expanding the certification requirement "could promote transparency and improve the consistency of the data contained in the database."[142] Like the expanded mitigation obligation above, this approach will ensure that every provider in the call chain is covered by the same basic set of rules and will increase transparency and accountability. We also agree with USTelecom that requiring non-gateway intermediate providers to file a certification and mitigation

(Continued from previous page)
referencing those providers "without" a STIR/SHAKEN implementation obligation, we mean those providers that are subject to an implementation extension, such as a provider with an entirely non-IP network or one that is unable to obtain the necessary SPC token to authenticate caller ID information, or that lack control over the facilities necessary to implement STIR/SHAKEN. *See* 47 CFR § 64.6304 (extension of implementation deadline).

[134] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1902, para. 82 (citation omitted).

[135] *Id.* (citations omitted); *see supra* para. 29.

[136] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1868, para. 19 (citing *First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3260, para. 40); *see supra* para. 29.

[137] *Fifth Caller ID Authentication Further Notice* at 75, para. 195.

[138] *Id.* at 79, para. 205.

[139] *Id.* at 75-76, para. 197.

[140] *Id.* at 77, para. 201.

[141] CCA Comments at 10; INCOMPAS Comments at 15-17 (arguing for a broad Robocall Mitigation Database filing obligation, including by those that do not have the facilities necessary to implement STIR/SHAKEN); NCTA Comments at 3; Professional Association for Customer Engagement (PACE) Comments at 4 (arguing that a Robocall Mitigation Database filing requirement for intermediate providers will "create[e] uniformity across provider-types and network segments"); USTelecom Comments at 8; VON Comments at 4; State AGs Reply at 10-11; TransNexus Reply at 12.

[142] ACA Connects Reply at 2-3 (discussing a certification requirements "for providers lacking control over the infrastructure necessary to implement STIR/SHAKEN (e.g., voice resellers)," and noting that "many such providers already filed voluntarily").

plan in the Robocall Mitigation Database will facilitate our enforcement efforts for those providers,[143] as it will for voice service providers newly obligated to file a mitigation plan.

39. Consistent with our proposal[144] and existing providers' obligations, all providers' robocall mitigation plans must describe the specific "reasonable steps" the provider has taken to avoid, as applicable, the origination, carrying, or processing of illegal robocall traffic as part of its robocall mitigation program.[145] A provider that plays more than one "role" in the call chain should explain the mitigation steps it undertakes in each role, to the extent those mitigation steps are different.[146]

40. *New Robocall Mitigation Program Description Obligations for All Providers*. Under the Commission's current rules, voice service providers are required to describe the specific "reasonable steps" that they have taken "to avoid originating illegal robocall traffic" as part of their robocall mitigation programs.[147] Gateway providers are required to address this topic and provide a description of how they have complied with the know-your-upstream provider requirement in section 64.1200(n)(4) of the Commission's rules.[148] We now impose specific additional requirements for the contents of robocall mitigation plans filed in the Robocall Mitigation Database.[149] Specifically, as part of their obligation to "describe with particularity" their robocall mitigation techniques, (1) voice service providers must describe how they are meeting their existing obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls;[150] (2) non-gateway intermediate providers and voice service providers must, like gateway providers, describe any "know-your-upstream provider" procedures in place designed to mitigate illegal robocalls;[151] and (3) all providers must describe any call analytics systems they use to identify and block illegal traffic, including whether they use a third-party vendor or vendors and the name of the vendor(s).[152] To comply with the new requirements to describe

[143] USTelecom Reply at 7 ("For example, a provider identified in tracebacks as accepting significant volumes of illegal traffic from one or more providers with late and/or suspiciously recent entries to the RMD may be indicative of substandard due diligence efforts. Downstream providers that accept traffic from [Robocall Mitigation Database] filers that submit incomplete or incomprehensible robocall mitigation plans, or that include inconsistencies or other questionable information in their . . . filings, may too be indicative of a problem worthy of Commission scrutiny.").

[144] *See Fifth Caller ID Authentication Further Notice* at 76, para. 195, 197.

[145] *See* 47 CFR § 64.6305(c)(2)(ii), (d)(ii).

[146] *See infra* para. 44 (revising the Commission's rules to require all providers to submit additional information regarding their role(s) in the call chain in robocall mitigation plans); *Fifth Caller ID Authentication Further Notice* at 76, para. 198 (proposing that, as part of the Bureau's delegated authority to specify the form and format of any submissions, providers amending their current plan to cover different roles in the call path explain the mitigation steps they undertake as one type of provider and what mitigation steps they undertake as a different type of provider, to the extent they are different).

[147] 47 CFR § 64.6305(c)(2)(ii).

[148] 47 CFR § 64.6305(d)(2)(ii); *see also id.* § 64.1200(n)(4) ("A voice service provider must . . . [i]f the provider acts as a gateway provider, take reasonable and effective steps to ensure that any foreign originating provider or foreign intermediate provider from which it directly receives traffic is not using the gateway provider to carry or process a high volume of illegal traffic onto the U.S. network.").

[149] *See Fifth Caller ID Authentication Further Notice* at 78, para. 203 (seeking comment on the specific areas or topics to be described in mitigation plans submitted to the Robocall Mitigation Database).

[150] 47 CFR § 64.1200(n)(3). We do not expect providers to necessarily submit contractual provisions, but to describe them in general terms, including whether such provisions are typically included in their contracts.

[151] While we do not currently require intermediate providers other than gateway providers to engage in "know-your-upstream provider" procedures, if they have put such procedures in place, they must be documented in their robocall mitigation plan.

[152] While we do not specifically require providers to use call analytics as EPIC/NCLC urges, *see* EPIC/NCLC Comments at 12 (arguing that a provider should not be able to evade liability under the reasonable steps standard by (continued….)

their "new and renewing customer" and "know-your-upstream provider" procedures, providers must describe any contractual provisions with end-users or upstream providers designed to mitigate illegal robocalls.[153] We conclude that the obligation to describe these procedures is particularly important for voice service providers without a STIR/SHAKEN implementation obligation.[154]

41. We impose these new requirements because it has become increasingly clear that provider due diligence and the use of call analytics are key ways to stop illegal robocalls.[155] The public and the Commission's understanding of the steps providers take to scrutinize their relationships with other providers in the call path and analyze their traffic will facilitate compliance with and enforcement of our rules.[156] Recent actions by the Enforcement Bureau demonstrating that some providers are not

(Continued from previous page)
asserting that it did not have the tools to monitor call traffic), doing so may be a "reasonable step" to mitigate illegal robocall traffic, depending on the circumstances. For example, if a provider is a reseller, it is likely to rely on any analytics software adopted by its wholesale provider to monitor call traffic. In that case, the reseller should describe this practice in its robocall mitigation plan.

[153] INCOMPAS Comments at 15-16.

[154] CCA Comments at 12-13 (arguing that resellers exempt from implementing STIR/SHAKEN are in the "best position to vet new customers" and should be required to file in the Robocall Mitigation Database and describe their "know-your-customer" process if they serve end-users). In the *Gateway Provider Order*, we required gateway providers to comply with a new requirement to "know" their upstream provider and required gateway providers to include in their Robocall Mitigation Database-filed mitigation plan a description of how it has complied with this obligation. *Gateway Provider Order* at 17, para. 37; 47 CFR § 64.6305(d)(2)(ii). In the *Fifth Caller ID Authentication Further Notice*, we sought comment on expanding these two requirements to non-gateway intermediate providers. *See Fifth Caller ID Authentication Further Notice* at 70-71, paras. 183-86. We continue to study the record on whether to do so. Similarly, we continue to consider whether to adopt our proposal to require all providers to respond to traceback requests within 24 hours as gateway providers are currently required to do. *See id.* at 69, para. 177.

[155] *See, e.g.*, CCA Comments at 8-9 ("Most providers routinely engage in some level of due diligence in the customer acquisition and onboarding process. . . . A compliant robocall mitigation plan should include at least this level of customer due diligence."); Credit Union National Association et al. (CUNA) Comments at 2; EPIC/NCLC Comments at 12 (citing NCLC, Scam Robocalls: Telecom Providers Profit at 16-18 (June 1, 2022), https://www.nclc.org/resources/scam-robocalls-telecom-providers-profit/) (arguing that taking "reasonable steps" should include call analytics and possibly also content analytics); ZipDX Comments at 4; Letter from Joshua M. Bercu, Executive Director, ITG, to Marlene H. Dortch, Secretary, FCC, GC Docket No. 17-59, WC Docket No. 17-97, at 3-5 (filed Sept. 1, 2022) (ITG Sept 1 *Ex Parte*).

[156] Verizon Reply at 1 (arguing that the Commission should support "emerging industry-driven innovations, such as [know-your-customer] tools that service providers can use to establish a 'chain of trust' between callers and recipients as well as to facilitate compliance with the Commission's robocall mitigation rules); *see also* CCA Comments at 5; USTelecom Comments at 5.

including meaningful descriptions in their mitigation plans warrants more prescriptive obligations.[157] There is also specific record support for these new requirements.[158]

42. *Baseline Information Submitted with Robocall Mitigation Database Certifications*. Consistent with existing providers' filing obligations and our proposal in the *Fifth Caller ID Authentication Further Notice*, all providers newly obligated to submit a certification to the Robocall Mitigation Database pursuant to the requirements adopted herein must submit the following information: (1) whether it has fully, partially, or not implemented the STIR/SHAKEN authentication framework in the IP portions of its network; (2) the provider's business name(s) and primary address; (3) other business name(s) in use by the provider; (4) all business names previously used by the provider; (5) whether the provider is a foreign provider; and, (6) the name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues.[159] The certification must be signed by an officer of the company.[160] Consistent with our proposal and current rules, providers with a new filing obligation must update any information submitted within 10 business days of "any change in the information" submitted, ensuring that the information is kept up to date.[161] Certifications and robocall mitigation plans must be submitted in English or with a certified English translation.[162]

43. *Additional Information to be Submitted with Mitigation Plans.* In order to effectively implement our new and modified authentication obligations, in addition to the baseline information

[157] *See, e.g.*, *Akabis, LLC*, Order, DA 22-1032, at 3, paras. 5-7 (EB Oct. 3, 2022) (finding provider filed deficient certification because its robocall mitigation plan consisted only of "a slide that appears to have been created by a third party, Inteliquent, describing the process to obtain a STIR/SHAKEN certificate" rather than a description of "reasonable steps"); *Cloud4 Inc.*, Order, DA 22-1038, at 3, paras. 5-7 (EB Oct. 3, 2022) (finding provider filed deficient certification because its robocall mitigation plan consisted only of a request for confidentiality); *Global UC Inc.*, Order, DA 22-1037, at 3, paras. 5-7 (EB Oct. 3, 2022) (deficient mitigation plan consisting only of background technical information) (*Global UC Notice Order*); *Horizon Technology Group LLC*, Order, DA 22-1036, at 3, paras. 5-7 (EB Oct. 3, 2022) (deficient mitigation plan consisting only of screenshot of Commission website); *Morse Communications Inc.*, Order, DA 22-1035, at 3, paras. 5-7 (EB Oct. 3, 2022); *Sharon Telephone Company*, Order, DA 22-1034, at 3, paras. 5-7 (EB Oct. 3, 2022); *Southwest Arkansas Telecommunications and Technology, Inc.*, Order, DA 22-1033, at 3, paras. 5-7 (EB Oct. 3, 2022) (all on file in EB-TCD-22-00033932).

[158] *See, e.g.*, CCA Comments at 13 (supporting a requirement that resellers describe their know-your-customer process); INCOMPAS Comments at 15-16 (supporting a requirement that providers describe their know-your-customer process); VON Comments at 8 & n.16; TransNexus Reply at 13 ("The Commission should require certifying providers to describe in sufficient detail how they vet customers and upstream providers and monitor traffic.").

[159] *Fifth Caller ID Authentication Further Notice* at 75, para. 197 (citing 47 CFR § 64.6305).

[160] *Cf.* 47 CFR § 64.6305(c)(3)(ii) (obligation for voice service providers); *id.* § 64.6305(d)(3)(ii) (obligation for gateway providers); *id*. § 1.16.

[161] *See Fifth Caller ID Authentication Further Notice* at 76, para. 199; 47 CFR § 64.6305(c)(5) ("A voice service provider shall update its filings within 10 business days of any change to the information it must provide pursuant to paragraphs (c)(1) through (4) of this section."); *id*. § 64.6305(d)(5) (parallel obligation for gateway providers).

[162] *Cf*. 47 CFR § 64.6305(c)(2) (obligation for voice service providers); *id.* § 64.6305(d)(2) (obligation for gateway providers); *see also Gateway Provider Order* at 17-18, para. 38; 47 CFR § 1.355 ("Every document, exhibit, or other paper written in a language other than English, which shall be filed in any proceeding, or in response to any order, shall be filed in the language in which it is written together with an English translation thereof duly verified under oath to be a true translation. Each copy of every such document, exhibit, or other paper filed shall be accompanied by a separate copy of the translation."); *id*. § 63.53(c) ("Applications submitted under Section 214 of the Communications Act [of 1934, as amended] for international services and any related pleadings that are in a foreign language shall be accompanied by a certified translation in English."); *U.S. v. Rivera-Rosario*, 300 F.3d 1, 5 (1st Cir. 2002) ("It is clear, to the point of perfect transparency, that federal court proceedings must be conducted in English.").

currently required of all filers, we also require providers to submit additional information in their Robocall Mitigation Database certifications.[163] We require all providers: (1) to submit additional information regarding their role(s) in the call chain; (2) asserting they do not have an obligation to implement STIR/SHAKEN to include more detail regarding the basis of that assertion; (3) to certify that they have not been prohibited from filing in the Robocall Mitigation Database; and (4) to state whether they are subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing and provide information concerning any such actions or investigations.

44. First, to increase transparency for the industry and regulators and better facilitate our evaluation of the mitigation plans detailed in the Robocall Mitigation Database, we require providers to submit additional information to indicate the role or roles they are playing in the call chain. Specifically, providers must indicate whether they are: (1) a voice service provider with a STIR/SHAKEN implementation obligation serving end-users; (2) a voice service provider with a STIR/SHAKEN obligation acting as a wholesale provider originating calls; (3) a voice service provider without a STIR/SHAKEN obligation; (4) a non-gateway intermediate provider with a STIR/SHAKEN obligation; (5) a non-gateway intermediate provider without a STIR/SHAKEN obligation; (6) a gateway provider with a STIR/SHAKEN obligation; (7) a gateway provider without a STIR/SHAKEN obligation; and/or (8) a foreign provider. This requirement expands upon the existing rule that providers indicate in their Robocall Mitigation Database filings whether they are a foreign provider, voice service provider, and/or gateway provider.[164] We note that certain provider classes have different obligations under our rules and, as explained above, the "reasonable steps" necessary to meet our mitigation standard may differ based on the provider's role in the call path. We conclude, therefore, that the collection of this information is necessary to allow the public and the Commission to determine whether a specific provider's mitigation steps are reasonable.

45. Second, we expand our requirement that providers with a current Robocall Mitigation Database filing obligation must state in their mitigation plan whether a STIR/SHAKEN extension applies,[165] and apply that rule to all current and new Robocall Mitigation Database filers. Specifically, a filer asserting it does not have an obligation to implement STIR/SHAKEN because of an ongoing extension, or because it lacks the facilities necessary to implement STIR/SHAKEN, must both explicitly state the rule that exempts it from compliance[166] and explain in detail why that exemption applies to the filer.[167] We conclude that this limited expansion of our existing rule is necessary to permit the public and Commission to evaluate why a provider believes it is not subject to all or a subset of our rules and whether that explanation is reasonable.

46. Third, we require new and existing filers to certify that they have not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action, including the new

[163] In the *Fifth Caller ID Authentication Further Notice*, we sought comment on whether some or all providers should submit additional information to the Robocall Mitigation Database. *See Fifth Caller ID Authentication Further Notice* at 75-76, 77-78, paras. 197-98, 201-203.

[164] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1903, para. 84; *Gateway Provider Order* at 17, para. 36.

[165] 47 CFR § 64.6305(c)(2)(i), (d)(2)(i).

[166] For example, by explaining that it lacks the necessary facilities to implement STIR/SHAKEN or it cannot obtain an SPC token. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1868, para. 19 (citing *First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3260, para. 40); *id.* at 1882-83, para. 50; 47 CFR § 64.6304.

[167] For example, by explaining that it is a pure reseller with some facilities, but that they are not sufficient to implement STIR/SHAKEN, or the steps it has taken to "diligently pursue" obtaining a token. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1882-83, para. 50.

enforcement requirements adopted herein.[168] Filers will be required to certify that they have not been barred from filing in the Robocall Mitigation Database by such an enforcement action. This includes, but is not limited to, instances in which a provider has been removed from the Robocall Mitigation Database and has been precluded from refiling unless and until certain deficiencies have been cured[169] and those in which a provider's authorization to file has been revoked due to continued violations of the Commission's robocall mitigation rules.[170] This information will enhance the effectiveness of the new enforcement measures we adopt herein to impose consequences on repeat offenders of our robocall mitigation rules.[171] We also adopt our proposal to require providers to submit information regarding their principals, affiliates, subsidiaries, and parent companies in sufficient detail to facilitate the Commission's ability to determine whether the provider has been prohibited from filing in the Robocall Mitigation Database.[172]

47. Fourth, we require all providers to: (1) state whether, at any time in the prior two years, the filing entity (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description; and, if so (2) provide a description of any such action or investigation, including all law enforcement or regulatory agencies involved, the date that any action or investigation was commenced, the current status of the action or investigation, a summary of the findings of wrongdoing made in connection with the action or investigation, and whether any final determinations have been issued.[173] We limit this reporting requirement to formal actions and investigations that have been commenced or issued pursuant to a written notice or other instrument containing findings by the law enforcement or regulatory agency that the filing entity has or is suspected of the illegal activities itemized above, including, but not limited to, notices of apparent liability, forfeiture orders, state or federal civil lawsuits or criminal indictments, and

[168] *See infra* Section III.C (adopting additional enforcement measures for violations of the Commission's robocall mitigation rules).

[169] *See October 2022 Robocall Mitigation Database Compliance/Removal Orders*, EB-TCD-22-00034406, Public Notice, DA 22-1220, at 2 (EB Nov. 22, 2022) (directing that the filer removed from the Robocall Mitigation Database "shall not refile until and unless the Wireline Competition Bureau and the Enforcement Bureau determine that [the filer] has addressed and resolved any deficiencies or shortcomings in its Robocall Mitigation Database certification") (*Removal Order*).

[170] *See infra* paras. 65-73 (defining when entities may be subject to revocations of section 214 authority and other Commission authorizations based on continued violations of the Commission's robocall mitigation rules).

[171] *See id*. We disagree with CCA that the same purpose can be served by indicating whether a provider filed under a prior name. CCA Comments at 10. This is not sufficient information to facilitate our rule barring related entities of repeated bad actors from filing in the Robocall Mitigation Database.

[172] *See Fifth Caller ID Authentication Further Notice* at 78, para. 201; *infra* paras. 71-73. Consistent with the delegation to the Wireline Competition Bureau to determine the form and format of providers' filings, *see infra* para. 52, we delegate to the Wireline Competition Bureau to determine the form and format of such data. *See infra* para. 73.

[173] In the *Fifth Caller ID Authentication Further Notice*, we sought comment on whether to adopt a requirement for providers to inform the Commission through an update to their Robocall Mitigation Database filing if the provider is subject to a Commission, law enforcement, or regulatory agency action, investigation, or inquiry due to its robocall mitigation plan being deemed insufficient or problematic, or due to suspected unlawful robocalling or spoofing. *Fifth Caller ID Authentication Further Notice* at 76, para. 199. We note that similar requirements for VoIP providers remain pending in the Direct Access proceeding. *See Numbering Policies for Modern Communications et al.*, WC Docket No. 13-97 et al., Further Notice of Proposed Rulemaking, 36 FCC Rcd 12907, 12914-15, para. 15 (2021) (*Direct Access Further Notice*).

cease-and-desist notices.[174] This information will help the Commission evaluate claims made by providers in their mitigation program descriptions and identify potential violations of our rules. We agree with commenters, however, that providers should not be required to submit information concerning mere inquiries from law enforcement or regulatory agencies or investigations that do not include findings of actual or suspected wrongdoing.[175] Thus, for example, traceback requests,[176] Enforcement Bureau letters of inquiry or subpoenas, or investigative demand letters or subpoenas issued by regulatory agencies or law enforcement would not trigger this obligation because they are not accompanied by findings of actual or suspected wrongdoing. We find that inquiries or investigations that do not contain findings of actual or suspected wrongdoing by the law enforcement or regulatory agency would be of limited value to the Commission in evaluating the certifications and robocall mitigation plans submitted to the Robocall Mitigation Database.[177]

48. Finally, we require filers to submit their OCN if they have one.[178] An OCN is a prerequisite to obtaining an SPC token, and we conclude that filing the OCN or indicating that they do not have one will allow us to more easily determine whether a provider is meeting its requirement to diligently pursue obtaining a token in order to authenticate their own calls and provides an additional way to determine relationships among providers. We do not require filers to include additional identifying information discussed in the *Gateway Provider Further Notice*.[179] There was no support for doing so, and we find the incremental benefits of providing additional information beyond the OCN are unclear.[180]

49. *Robocall Mitigation Database Filing Deadlines*. Providers newly subject to our Robocall Mitigation Database filing obligations must submit a certification and mitigation plan to the Robocall Mitigation Database by the later of: (1) 30 days following publication in the Federal Register of notice of approval by the Office of Management and Budget (OMB) of any associated Paperwork Reduction Act (PRA) obligations; or (2) any deadline set by the Wireline Competition Bureau through Public Notice. This approach provides additional flexibility to the Wireline Competition Bureau to provide an extended

[174] Providers that must include confidential information to accurately and fully comply with this reporting requirement, as explained below, may seek confidential treatment of that information pursuant to section 0.459 of the Commission's rules. 47 CFR § 0.459. *See infra* para. 49.

[175] *See* VON Comments at 6 (arguing that providers should not be required to submit information regarding inquiries about alleged robocall traffic).

[176] INCOMPAS Reply at 5 (arguing that "the number of traceback requests that a provider receives is not indicative of its responsibility for illegal robocall campaigns" (citing ITG Sept 1 *Ex Parte* at 6)); ITG Sept 1 *Ex Parte* at 6 ("Absent proper context and appropriate investigation, raw traceback data can understate the complicity of purposefully evasive bad actors while at the same time incorrectly stating or overstating the responsibility of a voice provider, including lesser-known small providers.").

[177] *See, e.g.*, Robocall Facilitators Must Cease and Desist, FCC (2023), https://www.fcc.gov/robocall-facilitators-must-cease-and-desist (last visited Feb. 8, 2023).

[178] *Gateway Provider Further Notice*, 36 FCC Rcd at 15005, para. 100 (seeking comment on whether the Commission should collect providers' OCN); ZipDX Comments at 13 (arguing that the OCN should be collected).

[179] *Gateway Provider Further Notice*, 36 FCC Rcd at 15005, para. 100 (in addition to their OCN, seeking comment on whether we should require filers to provide their Carrier Identification Code and/or Access Customer Name Abbreviation); *see also* CCA Comments at 10 (opposing requiring providers to file additional information).

[180] INCOMPAS Comments at 16 (arguing that the "additional information requirements suggested by the Commission may be unnecessarily burdensome and are unlikely to enhance compliance"). We also do not adopt TransNexus's proposal for providers to submit their registration information from the STI-GA website. TransNexus Reply at 13-14. We conclude that while such information may be helpful in determining whether a provider is participating in STIR/SHAKEN, reliance on the posting on a third-party website may complicate compliance (for example, if the STI-GA alters its website or modifies the information it chooses to post).

filing window where circumstances warrant.[181] Existing filers subject to new or modified requirements adopted in this *Sixth Report and Order* must amend their filings with the newly required information by the same deadline. If a provider is required to fully implement STIR/SHAKEN but has not done so by the Robocall Mitigation Database filing deadline, it must so indicate in its filing. It must then later update the filing within 10 business days of completing STIR/SHAKEN implementation.[182] We recognize that some of this information may be considered confidential. Providers may make confidential submissions consistent with our existing confidentiality rules.[183]

50. *Refusing Traffic From Unlisted Providers*. As proposed, we extend the prohibition on accepting traffic from unlisted (including de-listed) providers to non-gateway intermediate providers.[184] This proposal is well supported in the record and will close the final gap in our Robocall Mitigation Database call blocking regime.[185] Under this rule, downstream providers will be prohibited from accepting any traffic from a non-gateway intermediate provider not listed in the Robocall Mitigation Database, either because the provider did not file or their certification was removed as part of an enforcement action.[186] We conclude that a non-gateway intermediate provider Robocall Mitigation Database filing requirement and an associated prohibition against accepting traffic from non-gateway intermediate providers not in the Robocall Mitigation Database will ensure regulatory symmetry. By extending this prohibition to non-gateway intermediate providers, we ensure that downstream providers will no longer be required to determine the "role" of the upstream provider on a call-by-call basis to determine whether the call should be blocked.[187] Consistent with our proposal, and the parallel requirements adopted for accepting traffic from gateway providers and voice service providers, compliance will be required no sooner than 90 days following the deadline for non-gateway intermediate providers to submit a certification to the Robocall Mitigation Database.[188]

---

[181] ACA Connects Comments at 7 (asking for a deadline of no earlier than six months following approval of the relevant information collection obligations); State AGs Reply at 11 (asking for the Commission to adopt the shortest proposed compliance deadlines).

[182] *See* 47 CFR § 64.6305(c)(5) (requirement for voice service providers); *id.* § 64.6305(d)(5) (requirement for gateway providers).

[183] *Wireline Competition Bureau Adopts Protective Order for Robocall Mitigation Program Descriptions*, WC Docket No. 17-97, Public Notice, Attach. (Protective Order), 36 FCC Rcd 14562, 14566, para. 2 (WCB 2021) (defining confidential information filed as part of a robocall mitigation plan as information filed consistent with the Protective Order or sections 0.459 or 0.461 of the Commission's rules) (*Protective Order Public Notice*). As USTelecom noted previously, providers may only redact filings to the extent appropriate under our confidentiality rules. *See* USTelecom *Gateway Provider Further Notice* Comments at 8-9; *Protective Order Public Notice*, 36 FCC Rcd at 414565 ("[F]ilings which are overly redacted are not appropriate . . . . We will not hesitate to act should we identify improper confidentiality requests.").

[184] *See Fifth Caller ID Authentication Further Notice* at 79, para. 205.

[185] Comcast Comments at 11 (arguing that it would be a "natural extension of this obligation once intermediate providers are required to submit a Database certification"); NYPSC Comments at 1-2; USTelecom Reply at 5-6; ZipDX *Gateway Provider Further Notice* Comments at 32-33 (arguing that all providers should be required to file in the Robocall Mitigation Database and have their traffic blocked if they are not listed); *see also* USTelecom Comments at 8-9 (arguing for a database filing obligation for all intermediate providers); Verizon *Gateway Provider Further Notice* Reply at 5.

[186] *See, e.g., Removal Order* at 2-3.

[187] USTelecom Reply at 5 (arguing that the intermediate provider blocking rule would "simplif[y] the Commission's regime" so that the Commission's rules would "simply prohibit any provider from accepting traffic from any other provider that has not certified to its robocall mitigation practices in the [Robocall Mitigation Database]").

[188] *See Fifth Caller ID Authentication Further Notice* at 79, para. 206.

51. As a result of non-gateway intermediate providers' affirmative obligation to submit a certification in the Robocall Mitigation Database, downstream providers may not rely upon any non-gateway intermediate provider database registration imported from the intermediate provider registry.[189] Any imported Robocall Mitigation Database entry is not sufficient to meet a non-gateway intermediate provider's Robocall Mitigation Database filing obligation or to prevent downstream providers from blocking traffic upon the effective date of the obligation for downstream providers to block traffic from non-gateway intermediate providers.

52. *Bureau Guidance*. Consistent with the Commission's prior delegations of authority concerning the Robocall Mitigation Database submission process,[190] we direct the Wireline Competition Bureau to make the necessary changes to the Robocall Mitigation Database and to provide appropriate Robocall Mitigation Database filing instructions and training materials as necessary and consistent with this Report and Order. We delegate to the Wireline Competition Bureau the authority to specify the form and format of any submissions as well as necessary changes to the Robocall Mitigation Database submission interface. We also delegate to the Wireline Competition Bureau the authority to make the necessary changes to the Robocall Mitigation Database to indicate whether a non-gateway intermediate provider has made an affirmative filing (as opposed to being imported as an intermediate provider) and whether any provider's filing has been de-listed as part of an enforcement action, and to announce its determination as part of its guidance. We also direct the Wireline Competition Bureau to release a public notice upon OMB approval of any information collection associated with our Robocall Mitigation Database filing requirements, announcing OMB approval of our rules, effective dates, and deadlines for filing and for providers to block traffic from non-gateway intermediate providers that have not filed.

C. Enforcement

53. In order to further strengthen our efforts to hold illegal robocallers accountable for their actions, we adopt several enforcement proposals described in the *Fifth Caller ID Authentication Further Notice*.[191] Specifically, we: (1) adopt a per-call forfeiture penalty for failure to block traffic in accordance with our rules and set maximum forfeitures for such violations; (2) require the removal of non-gateway intermediate providers from the Robocall Mitigation Database for violations of our rules, consistent with the standard applied to other filers; (3) establish an expedited process for provider removal for facially deficient certifications; and (4) establish rules that would impose consequences on repeat offenders of our robocall mitigation rules. The adoption of more robust enforcement tools is supported in the record.[192] As USTelecom notes, strong enforcement action can significantly reduce the prevalence of illegal robocall campaigns.[193]

---

[189] *See id.* at 79, para. 205. Previously, all intermediate providers were imported into the Robocall Mitigation Database from the rural call completion database's Intermediate Provider Registry so that all intermediate providers would be represented therein, giving voice service providers "confidence that any provider not listed in the Robocall Mitigation Database" was not in compliance with the Commission's rules. *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1904, para. 87 n.340.

[190] *See, e.g.*, *Gateway Provider Order* at 21, paras. 39, 45, 47-48 (delegating to the Wireline Competition Bureau the authority to specify the form and format of gateway provider submissions and to make necessary changes to the Robocall Mitigation Database and portal, and directing the Wireline Competition Bureau to provide filing instructions and to release a public notice setting deadlines and announcing its determinations regarding the management of imported and de-listed filings); *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1902-903, para. 83 (directing the Wireline Competition Bureau to establish the Robocall Mitigation Database and portal, to provide appropriate filing instructions and training materials, and to release a Public Notice when voice service providers may begin filing certifications).

[191] *See Fifth Caller ID Authentication Further Notice* at 80, para. 207.

[192] *See generally* CCA Comments at 2 (advocating for strong enforcement steps); USTelecom Comments at 7 (same); ACA Connects Reply at 3 (same); Verizon Reply at 1 (same); *see also* NCTA Comments at 4 (writing that (continued….)

1. Per Call Maximum Forfeitures

54. We first adopt our proposal to establish a forfeiture penalty on a per-call basis for violations of our robocall blocking rules in 47 CFR § 64.1200 *et seq.*[194] and 47 CFR § 64.6300 *et seq*.[195] Commenters generally agreed that aggressive penalties are appropriate.[196] Mandatory blocking is an important tool for protecting American consumers from illegal robocalls.[197] As we have found in our previous robocalling orders and enforcement actions, illegal robocalls cause significant consumer harm.[198] Penalties for failure to comply with mandatory blocking requirements must deter noncompliance and be sufficient to ensure that entities subject to these requirements are unwilling to risk suffering serious economic harm.

55. Consistent with our proposal, we authorize the maximum forfeiture amount for each violation of the mandatory blocking requirements of $23,727 per call.[199] This is the maximum forfeiture amount our rules permit us to impose on non-common carriers.[200] Although common carriers may be assessed a maximum forfeiture of $237,268 for each violation,[201] we find that we should not impose a greater penalty on one class of providers than another for purposes of the mandatory blocking requirements. We also set a base forfeiture amount of $2,500 per call because we conclude that the failure to block results in a similar consumer harm as the robocall itself (e.g., the consumer receives the robocall itself). We find that a $2,500 base forfeiture is reasonable in comparison to the $4,500 base

(Continued from previous page)
"[s]trong enforcement of the Commission's call authentication and blocking rules is essential to protecting the public"); ZipDX Comments at 14.

[193] *See* USTelecom Comments at 15.

[194] *See* 47 CFR §§ 64.1200(n)(5) (requiring gateway providers to block illegal traffic following Commission notice); § 64.1200(n)(6) (requiring providers to block traffic from an immediately upstream gateway provider that itself has failed to block pursuant to (n)(5)); § 64.1200(o) (requiring gateway providers to block calls sent from a number on a "reasonable do-not originate list").

[195] 47 CFR § 64.6305(e); Appx. A § 64.6305(g) (requiring providers to not accept traffic from upstream providers not in the robocall mitigation database).

[196] *See* CCA Comments at 11 (while supporting the application of relevant mitigating and aggravating factors where appropriate, agreeing that maximum penalties are appropriate for bad actors); NCTA Comments at 4 (stating that "NCTA does not oppose the penalties proposed" but suggesting that the Commission adopt a "good faith" standard when imposing forfeitures); ZipDX Comments at 14 (agreeing that "penalties should be on a per-call basis").

[197] *Fifth Caller ID Authentication Further Notice* at 331, para. 73.

[198] *See, e.g.*, *Gateway Provider Order* at 3, para. 5; *John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, Forfeiture Order, 36 FCC Rcd 6225, 6237-39, paras. 26-29 (2021) (*Rising Eagle Forfeiture Order*); *Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, 33 FCC Rcd 4663, 4668, para. 15 (2018) (*Abramovich Forfeiture Order*).

[199] *Fifth Caller ID Authentication Further Notice* at 80, para. 209. We note that the maximum forfeiture amounts have increased since the adoption of the *Fifth Caller ID Authentication Further Notice*, which sought comment on a maximum $22,021 forfeiture amount. *Amendment of Section 1.80(b) of the Commission's Rules et al.,* Order, DA 22-1356 at 1, para. 1 (EB Dec. 23, 2022) ("This Order amends section 1.80(b) of the Commission's rules to adjust the forfeiture penalties for inflation . . . ."); *id*. Appx. A § 1.80(b)(9) (setting maximum forfeiture for violations "for any case not previously covered" at $23,727).

[200] 47 CFR § 1.80(b)(9).

[201] *Id.* § 1.80(b)(2).

forfeiture for violations of the Telephone Consumer Protection Act of 1991 (TCPA).[202] While the failure to block produces significant consumer harm, the harm is not as great and does not carry the same degree of culpability as the initiator of an illegal robocall campaign who may have committed a TCPA violation. While we sought comment on whether we should consider specific additional mitigating or aggravating factors, we did not receive sufficient comment to provide a basis for doing so.[203] As with other violations of our rules, however, existing upward and downward adjustment criteria in section 1.80 of the Commission's rules may apply.[204] Additionally, there may be pragmatic factors in our prosecutorial discretion in calculating the total forfeiture amount—particularly when there is a very large number of calls at issue—as we have done in our enforcement actions pursuant to the TCPA and those actions taken against spoofing.[205]

2. Provider Removal from the Robocall Mitigation Database

56. We also adopt our proposal to provide for the removal of non-gateway intermediate providers from the database for violations of our rules.[206] In the *Second Caller ID Authentication Report and Order*, the Commission set forth consequences for voice service providers that file a deficient robocall mitigation plan or that "knowingly or negligently" originate illegal robocall campaigns, including removal from the Robocall Mitigation Database.[207] Gateway providers are now subject to the same rules for calls that they carry or process.[208] To promote regulatory symmetry, we conclude that non-gateway intermediate providers should face similar consequences.[209]

57. Specifically, we find that a non-gateway intermediate provider with a deficient certification—such as when the certification describes a program that is unreasonable, or if we determine that a provider knowingly or negligently carries or processes illegal robocalls—we will take appropriate enforcement action.[210] This may include, among other actions, removing a certification from the database after providing notice to the intermediate provider and an opportunity to cure the filing, requiring the intermediate provider to submit to more specific robocall mitigation requirements, and/or proposing the imposition of a forfeiture. We decline, however, to adopt other reasons to remove providers from the database. We conclude that the existing basis for removal is appropriately tailored to the underlying purpose of the Robocall Mitigation Database—to facilitate detection and elimination of illegal robocall

---

[202] *Sumco Panama SA et al.*, Notice of Apparent Liability for Forfeiture, FCC 22-99, at 34, para. 77 (Dec. 23, 2022) ("The Commission has on multiple occasions used a base forfeiture of $4,500 for violations involving section 227(b) [and we] propose to follow that same approach here.").

[203] CCA Comments at 11 (stating that the Commission "should tailor penalties based on a variety of aggravating or mitigating factors[,]" including "the provider's history of compliance and responsiveness to traceback requests or other Commission notifications, reasonable steps the provider took to mitigate illegal traffic on its network, and the robustness of its mitigation plan and its implementation").

[204] 47 CFR § 1.80(b)(10) tbl. 3.

[205] *See Abramovich Forfeiture Order*, 33 FCC Rcd at 4665, para. 7 (using a sampling methodology); *John C. Spiller; Jakob A. Mears; Rising Eagle Capital Group LLC; Jsquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group – Cayman*, Notice of Apparent Liability, 35 FCC Rcd 5948, 5963-64, paras. 38-39 (2020) (*Spiller NAL*) (enumerating pragmatic factors); *Abramovich Forfeiture Order*, 33 FCC Rcd at 4671, para. 25 (upholding a forfeiture below the statutory maximum).

[206] *See Fifth Caller ID Authentication Further Notice* at 80, para. 210.

[207] *See Second Caller ID Authentication Report and Order,* 36 FCC Rcd at 1903, para. 83.

[208] *Gateway Provider Order* at 18, para. 40.

[209] *See Fifth Caller ID Authentication Further Notice* at 80, para. 210.

[210] *See id.* at 81, para. 210.

traffic.[211] As proposed, we explicitly expand our delegation of authority to the Enforcement Bureau to de-list or exclude a provider from the Robocall Mitigation Database to include the removal of non-gateway intermediate providers.[212]

58. Downstream providers must refuse traffic sent by a non-gateway intermediate provider that is not listed in the Robocall Mitigation Database, as described above and consistent with the existing safeguards applicable to our existing rules for refusing traffic for calls to 911, public safety answering points, and government emergency numbers.[213] We agree with VON that any sanctions for failure to block calls from a provider removed from the database should not occur without sufficient notice to the industry.[214] We conclude, however, that the existing Enforcement Bureau process, where providers are given two business days to block calls following Commission notice of removal from the database, is sufficient, as it appropriately balances the public's interest in blocking unwanted robocalls against the need to allow providers sufficient time to take the necessary steps to block traffic.[215]

3. Expedited Removal Procedure for Facially Deficient Filings

59. We agree with commenters that there are certain instances in which a provider should be removed from the Robocall Mitigation Database on an expedited basis.[216] Specifically, we find that where the Enforcement Bureau determines that a provider's filing is facially deficient, the Enforcement Bureau may remove a provider from the Robocall Mitigation Database using an expedited two-step procedure, which entails providing notice and an opportunity to cure the deficiency. This streamlined process will allow the Enforcement Bureau to move more quickly against providers whose filings clearly fail to meet our requirements.

60. In the *Second Caller ID Authentication Report and Order*, the Commission required that providers be given notice of any deficiencies in their certification and an opportunity to cure prior to removal from the Robocall Mitigation Database, but did not prescribe a specific removal procedure.[217] Pursuant to that requirement and our prior delegation, the Wireline Competition Bureau and Enforcement Bureau have implemented the following three-step removal procedure: (1) the Wireline Competition Bureau contacts the provider, notifying it that its filing is deficient, explaining the nature of the deficiency, and providing 14 days for the provider to cure the deficiency;[218] (2) if the provider fails to rectify the deficiency, the Enforcement Bureau releases an order concluding that a provider's filing is deficient based on the available evidence and directing the provider to explain, within 14 days, "why the Enforcement Bureau should not remove the Company's certification from the Robocall Mitigation

[211] There was limited comment on other bases of removal from the Robocall Mitigation Database, although we agree with several parties that the number of traceback requests is not a valid reason for removal. *See e.g.*, INCOMPAS Reply at 4; CCA Comments at 12. As explained below, we conclude that the number of traceback requests received should not serve as a basis for any sanction. *See infra* para. 74.

[212] *Fifth Caller ID Authentication Further Notice* at 81, para. 210.

[213] 47 CFR § 64.6305(e)(4) (public safety safeguards).

[214] VON Comments at 7.

[215] *See Global UC Inc*., EB-TCD-22-00034406, Removal Order, DA 22-1219, at 4, para. 8 (EB Nov. 22, 2022) (*Global UC Removal Order*) (requiring providers to cease accepting traffic from Global UC within two business days). Additionally, we have not received any complaints about this time period from providers required to block traffic following the removal of a provider from the database.

[216] *See* EPIC/NCLC Comments at 18-19; ZipDX Comments at 11-12.

[217] *Second Caller ID Authentication Order*, 36 FCC Rcd at 1903, para. 83.

[218] *See e.g.*, *Global UC Notice Order* at 2-3, para. 4 ("The FCC's Wireline Competition Bureau . . . contacted the Company on October 19, 2021, via the email listed in its certification, to inform it that its robocall mitigation program attachment contained with its certification may have been uploaded in error as it did not satisfy the Commission's rules to describe robocall mitigation efforts."); *id* at 3, para. 2.

Database" and giving the provider a further opportunity to cure the deficiencies in its filing;[219] and (3) if the provider fails to rectify the deficiency or provide a sufficient explanation why its filing is not deficient within that 14-day period, the Enforcement Bureau releases an order removing the provider from the Robocall Mitigation Database.[220]

61. While this procedure is appropriate in cases where there may be questions about the sufficiency of the steps described in a mitigation plan, we conclude that an expedited approach is warranted where the certification is facially deficient. A certification is "facially deficient" where the provider fails to submit a robocall mitigation plan within the meaning of our rules. That is, it fails to submit any information regarding the "specific reasonable steps" it is taking to mitigate illegal robocalls. While it is not practical to provide an exhaustive list of reasons why a filing would be considered "facially deficient," examples include, without limitation, instances where the provider only submits: (1) a request for confidentiality with no underlying substantive filing; (2) only non-responsive data or documents (e.g., a screenshot from the Commission's website of a provider's FCC Registration Number data or other document that does not describe robocall mitigation efforts); (3) information that merely states how STIR/SHAKEN generally works, with no specific information about the provider's own robocall mitigation efforts; or (4) a certification that is not in English and lacks a certified English translation. In these and similar cases, the Commission need not reach the question of whether the steps the provider is taking to mitigate robocalls are reasonable because the provider has failed to submit even the most basic information required to do so.

62. We conclude that where a provider's filing is facially deficient, it has "willfully" violated its Robocall Mitigation Database filing obligation within the meaning of that term in section 9(b) of the Administrative Procedure Act (APA), 5 U.S.C. § 558(c), which applies to revocations of licenses.[221] This finding is consistent with precedent concluding that a party acts "willfully" within the meaning of section 558(c) where it acts with "careless disregard."[222] As such, where a "willful" violation has occurred, the provider's Robocall Mitigation Database certification may be removed without a separate notice prior to the initiation of an "agency proceeding" to remove the certification.[223] Therefore, we adopt the following

---

[219] *Id*. at 3, para. 6.

[220] *See generally*, *Global UC Removal Order.*

[221] The term "license" is broadly defined under the APA to include "the whole or a part of an agency permit, certificate, approval, registration, charter, membership, statutory exemption or other form of permission." 5 U.S.C. § 551(8). Although we do not reach a definitive conclusion here, the removal of a provider's certification from the Robocall Mitigation Database—which will lead to the mandatory blocking of the provider's traffic by downstream providers—is arguably equivalent to the revocation of a license.

[222] *Coosemans Specialties, Inc. v. Dep't of Agric*., 482 F.3d 560, 567 (D.C. Cir. 2007) ("[A]n action [under 5 U.S.C. § 558(c)] is willful if a prohibited act is done intentionally, irrespective of evil intent, or done with careless disregard of statutory requirements.") (quoting *Finer Foods Sales Co. v. Block,* 708 F.2d 774, 778 (D.C. Cir. 1983)); *Potato Sales Co., Inc. v. Dep't. of Agric.*, 92 F.3d 800, 805 (9th Cir. 1996) ("In this circuit, a violation is 'willful' if the violator '(1) intentionally does an act which is prohibited, irrespective of evil motive or reliance on erroneous advice, or (2) acts with careless disregard of statutory requirements.'") (quoting *Lawrence v. Commodity Futures Trading Comm'n,* 759 F.2d 767, 773 (9th Cir. 1985)); *Goodman v. Benson*, 286 F.2d 896, 900 (7th Cir. 1961) ("We think it clear that if a person l) intentionally does an act which is prohibited, irrespective of evil motive or reliance on erroneous advice, or 2) acts with careless disregard of statutory requirements, the violation is wilful."); *see also Capital Produce Co., Inc. v. U.S.*, 930 F.2d 1077, 1079 (4th Cir. 1991) ("'[W]illfulness' for the purposes of Section 558(c) means an intentional misdeed or such gross neglect of a known duty as to be the equivalent thereof.") (internal quotations omitted).

[223] *See* 5 U.S.C. § 558(c) (holding that an agency may only withdraw or revoke a "license" through "an agency proceeding" if the agency has already provided "notice by the agency in writing of the facts or conduct which may warrant the action and an opportunity to demonstrate or achieve compliance with all lawful requirements" except "in cases of willfulness or those in which public health, interest or safety requires otherwise"). While we do not

(continued….)

two-step expedited procedure for removing a facially deficient certification: (1) issuance of a notice by the Enforcement Bureau to the provider explaining the basis for its conclusion that the certification is facially deficient and providing an opportunity for the provider to cure the deficiency or explain why its certification is not deficient within 10 days; and (2) if the deficiency is not cured or the provider fails to establish that there is no deficiency within that 10-day period, the Enforcement Bureau will issue an order removing the provider from the database.[224] We note that a number of providers have responded within 14 days to Enforcement Bureau requests to correct their deficient filings and conclude that employing a marginally shorter time period for this expedited process will further the Commission's interest in swiftly resolving these willful violations without materially affecting a providers' ability to respond to the Enforcement Bureau's notice.

63. We find that this expedited two-step procedure is also consistent with providers' Fifth Amendment due process rights under the Supreme Court's three factor test.[225] While providers have a significant "private interest" under the first factor of the test that would be affected by removal from the Robocall Mitigation Database, the "risk of an erroneous deprivation of such interest through the procedures used and the probable value, if any, of additional or substitute procedural safeguards" under the second factor is exceedingly low, given that (1) the filings in question are facially deficient, and (2) providers would have a reasonable opportunity to cure the deficient filings by submitting a valid robocall mitigation plan. Given the extremely low risk of erroneous deprivation of a private interest in these situations, we find that these first two factors do not outweigh the third factor—the "Government's interest"—which is very weighty here: the Government has a strong interest in ensuring that providers adopt valid robocall mitigation plans as soon as possible to further its continuing efforts to reduce the number of illegal robocalls and harm to consumers, and in blocking traffic of providers that are unable or unwilling to implement or document effective mitigation measures.[226]

64. We conclude that this expedited approach is preferable to EPIC/NCLC's proposal to automatically remove certain "high-risk" VoIP providers from the Robocall Mitigation Database or impose forfeitures through a bespoke, expedited process.[227] As explained above, we do not believe that a

(Continued from previous page)
specifically conclude that a Robocall Mitigation Database certification is a license within the meaning of that section, our expedited procedure would be compliant with section 558 if we reached such a conclusion.

[224] We also note that the Enforcement Bureau could adopt a similar two-step procedure in cases of "a threat to the public health, interest or safety." 5 U.S.C. § 558(c).

[225] *See Mathews v Eldridge*, 424 U.S. 319, 329-35 (1976) (concluding that a single notice and opportunity to respond prior to revocation of social security benefits was sufficient to meet Fifth Amendment due process requirements and an evidentiary hearing was not required under the three-factor due process test); *id*. at 334-35 ("[O]ur prior decisions indicate that identification of the specific dictates of due process generally requires consideration of three distinct factors: First, the private interest that will be affected by the official action; second the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail.").

[226] *Cf. China Telecom (Americas) Corp. v. FCC*, No. 21-1233, 2022 WL 18232291, at *9-11 (D.C. Cir. Dec. 20, 2022) (*China Telecom*) (holding that the first two factors did not outweigh the Government's interest with regard to the revocation of China Telecom's section 214 authorization).

[227] EPIC/NCLC Comments at 24 (urging the adoption of a temporary restraining order-like process). We disagree with EPIC/NCLC that because we required small non-facilities-based voice service providers to implement STIR/SHAKEN sooner that other voice service providers, we should similarly subject non-facilities-based VoIP providers to an expedited enforcement procedure. *Id*. at 18. The decision to require certain providers to implement STIR/SHAKEN on an accelerated timeline was based on an assessment of the likelihood of *future* rule violations and a balancing of the benefits and burdens of earlier implementation. *Small Provider Order* at 17844-46, paras. 10-13. EPIC/NCLC does not explain why a subset of providers should be subject to a separate enforcement process once the Commission determines a rule violation has likely occurred.

separate set of rules for VoIP providers is appropriate and the expedited procedure we adopt today complies with the APA and due process. EPIC/NCLC do not explain how removal from the database prior to any opportunity to respond is consistent with the APA or due process.

4. Consequences for Continued Violations

65. In order to address continued violations of our robocall mitigation rules, we proposed in the *Fifth Caller ID Authentication Further Notice* to subject repeat offenders to proceedings to "revoke their section 214 operating authority and to ban offending companies and/or their individual company owners, directors, officers, and principals from future significant association with entities regulated by the Commission."[228] We further proposed to find that providers that are not common carriers operating pursuant to blanket section 214 authority hold other Commission authorizations sufficient to subject them to the Commission's jurisdiction for purposes of enforcing our rules pertaining to preventing illegal robocalls.[229] We also proposed to find that providers not classified as common carriers but that are registered in the Robocall Mitigation Database hold a Commission certification such that they are subject to the Commission's jurisdiction.[230] We adopt our proposal to revoke the section 214 operating authority of entities that engage in continued violations of our robocall mitigation rules. We also find that non-common carriers holding Commission authorizations and/or certifications are similarly subject to revocation of their authorizations and/or certifications. We further find that we will consider whether it is in the public interest for individual company owners, directors, officers, and principals of entities for which we have revoked an authority or a certification, or for other entities with which those individuals are affiliated, to obtain future Commission authorizations, licenses, or certifications at the time that they apply for them.

66. *Revocation of Section 214 Authority and Other Commission Authorizations*. In the *Fifth Caller ID Authentication Further Notice*, we proposed to find that entities engaging in "continued violations of our robocall mitigation rules,"[231] be subject to revocation of their section 214 operating authority, where applicable.[232] We conclude that the "robocall mitigation rules" within the scope of this requirement means the specific obligations to: (1) implement a robocall mitigation program that includes specific "reasonable steps" to mitigate illegal robocalls and comply with the steps outlined in the plan; (2) submit a plan describing the mitigation program to the Robocall Mitigation database; and (3) not accept traffic from providers not in the Robocall Mitigation database.[233]

67. We conclude that this requirement also pertains to continued violation of providers' authentication obligations.[234] While in certain instances we have referred to provider mitigation obligations as separate from authentication, we have also concluded that they work hand in hand to stop illegal robocalls.[235] Indeed, analytics providers often use authentication information to determine whether

[228] *Fifth Caller ID Authentication Further Notice* at 79, para. 207.

[229] *Id.* at 81-82, para. 212.

[230] *Id.*

[231] *Id.* at 81, para. 211.

[232] *Id.*

[233] This includes obligations that the Commission previously adopted as well as those that we today in this *Sixth Report and Order*. 47 CFR § 64.6305; *infra* Appx. A § 64.6305.

[234] 47 CFR §§ 64.6301, 64.6302; *infra* Appx. A §§ 64.6301, 64.6302.

[235] *Gateway Provider Order* at 44-45, paras. 104-107 (concluding that authentication is not a "silver bullet" to stop robocalls, justifying requiring gateway providers to also mitigate robocalls under the "reasonable steps" standard).

to block or label a call.[236] We therefore conclude that call authentication serves to mitigate illegal robocalls, and failure to follow our authentication rules falls within the scope of the enforcement authority we adopt today.

68. We did not receive comments regarding the scope of the specific rules covered by the consequences proposed in the *Fifth Caller ID Authentication Further Notice*. We find, however, that it is reasonable to fully enforce the foregoing robocall mitigation rules by holding accountable those who engage in continued violations of those rules. We will exercise our ability to revoke the section 214 authorizations for providers engaging in continued violations of those rules, consistent with our long-standing authority to revoke the section 214 authority of any provider for serious misconduct. [237]

69. The Commission's authority to revoke section 214 authority in order to protect the public interest is well established.[238] We intend to apply that authority as necessary to address entities engaging in continued violations of our rules. Specifically, an entity engaging in continued violations of our robocall mitigation rules as defined in this section will be required to explain to the Enforcement Bureau why the Commission should not initiate proceedings to revoke its domestic and/or international section 214 authorizations.[239] Consistent with established Commission procedures, we may then adopt an order to institute a proceeding to revoke domestic and/or international section 214 authority.[240] Should the entity fail to address concerns regarding its retention of section 214 authority, we would then issue an Order on Revocation consistent with our authority to revoke section 214 authority when warranted to protect the public interest.[241]

70. We also adopt our proposals that providers not classified as common carriers but that hold other types of Commission authorizations, including a certification as a result of being registered in the Robocall Mitigation Database, are subject to the Commission's jurisdiction for the purpose of the consequences we adopt in this section.[242] The *Fifth Caller ID Authentication Further Notice* listed the

---

[236] Neustar *First Reevaluation of STIR/SHAKEN Extensions Public Notice* Reply at 4 (arguing that accurate attestation information levels "provide[s] terminating voice service providers with better information to inform robocall analytics services for protecting consumers from illegally spoofed robocalls").

[237] *See Implementation of Section 402(b)(2)(A) of the Telecomm. Act of 1996*, CC Docket No. 97-11, Report and Order & AAD File No. 98-43, Second Memorandum Opinion and Order, 14 FCC Rcd 11364, 11372, para. 12 (1999) (stating that the Commission, with the grant of blanket section 214 operating authority, retains the ability to stop "abusive practices against consumers by withdrawing the blanket section 214 authorization that allows the abusive carrier to operate"); *OneLink Communications, Inc. et al*., File No. EB-TCD-13-00007004 et al., Order to Show Cause, 32 FCC Rcd 1884, 1886, para. 8 (EB & WCB 2017) (initiating a proceeding to determine whether to revoke the domestic section 214 authorizations); *LDC Telecommunications, Inc*., File No.: ITC-214-20080523-00238, Revocation Order, 31 FCC Rcd 11661, 11662, para. 5 (EB, IB & WCB 2016) (revoking domestic and international section 214 authorizations for failure to pay regulatory fees and respond to multiple Commission inquiries).

[238] *See* 47 CFR § 0.91(q) (stating that the Wireline Competition Bureau may issue orders revoking a common carrier's operating authority); *China Telecom (Americas) Corp.*, GN Docket No. 20-109, Order on Revocation and Termination, 36 FCC Rcd 15966, 15968-70, 15975, 15977-83, paras. 4-5, 10-11, 14-22 (2021) (*China Telecom Order on Revocation*) (describing the Commission authority, applicable standard of proof, and public interest standard for revoking section 214 authority, including stating that the Commission has an ongoing responsibility to evaluate all aspects of the public interest in determining whether a provider is subject to revocation; also explaining revocation procedures), *aff'd*, *China Telecom (Americas) Corp. v. FCC*, No. 21-1233, 2022 WL 17814481 (D.C. Cir. 2022).

[239] *China Telecom Order on Revocation* at 15975, at para. 10 (describing Order to Show Cause).

[240] *Id.* at para. 11 (describing Institution Order).

[241] *Id.* at 15977, para. 14.

[242] *Fifth Caller ID Authentication Further Notice* at 81-82, para. 212 (stating that many providers that might engage in continued violations may not be classified as common carriers and thus may not operate subject to the blanket (continued….)

providers that we contemplated would be subject to our enforcement authority.[243] These providers have domestic and international section 214 authorizations, have applied for and received authorization for direct access to numbering resources,[244] are designated as eligible telecommunications carriers under section 214(e) of the Communications Act of 1934, as amended (Communications Act or Act) in order to receive federal universal service support,[245] or are registered in the Robocall Mitigation Database. Where the Commission grants a right or privilege, it unquestionably has the right to revoke or deny that right or privilege in appropriate circumstances.[246] In addition, holders of these and all Commission authorizations have a clear and demonstrable duty to operate in the public interest.[247] Continued violations of our robocall mitigation rules are wholly inconsistent with the public interest, and we find it necessary to exercise our authority to institute a proceeding and, if warranted, revoke the authorizations, licenses, and/or certifications of all repeat offenders,[248] Indeed, there is no opposition in the record to the Commission instituting revocation proceedings when warranted, and we agree with VON that when providers, including those without section 214 authority, have clearly and repeatedly been responsible for originating or transporting illegal robocalls and have had a sufficient opportunity to be heard through the

(Continued from previous page)
section 214 authority applicable to domestic interstate common carriers under section 63.01 of the Commission's rules, 47 CFR § 63.01). Interconnected VoIP providers are subject to Title II of the Act through their requirement to file applications to discontinue service under section 214 and section 63.71 of the Commission's rules. *IP-Enabled Services*, WC Docket No. 04-36, 24 FCC Rcd 6039, 6044-48, paras. 9-13 (2009). As explained below, this approach does not constitute an improper exercise of jurisdiction over domestic non-common carriers or foreign providers.

[243] *See Fifth Caller ID Authentication Further Notice* at 81-82, para. 212.

[244] *See Numbering Policies for Modern Communications et al.*, WC Docket No. 13-97 et al., Report and Order, 30 FCC Rcd 6839, 6878, para. 78 (2015), *appeal dismissed*, *NARUC v. FCC*, 851 F.3d 1324 (D.C. Cir. 2017).

[245] 47 U.S.C. § 251(e).

[246] *See, e.g.*, *Market Entry and Regulation of Foreign-Affiliated Entities*, IB Docket No. 95-22, 11 FCC Rcd 3873, 3887, para. 36 (1995) ("We recognize that our approach necessarily entails limiting the activities of certain competitors in U.S. markets. Specifically, we may prohibit foreign carriers (or their affiliates) that have market power from offering service along routes where they can exercise such power . . . . In our judgment, the benefits of allowing these foreign carriers unlimited access into the U.S. international services market are outweighed substantially by the ultimate costs."); *cf. Cable & Wireless P.L.C. v. FCC*, 166 F.3d 1224, 1230 (D.C. Cir. 1999) (finding that "the Commission does not exceed its authority simply because a regulatory action has extraterritorial consequences").

[247] *See* 47 U.S.C. § 214 (stating that no carrier shall undertake the construction of a new line or of an extension of any line, or shall acquire or operate any line, or extension thereof, or shall engage in transmission over or by means of such additional or extended line, unless and until there "shall first have been obtained from the Commission a certificate that the present or future public convenience and necessity" requires it); *id*. § 214(e)(6); 47 CFR §§ 54.202(b) (stating that prior to designating an eligible telecommunications carrier, the Commission must determine that such designation is in the public interest), 52.15(g)(iii) (stating that the Wireline Competition Bureau may halt the auto-grant of an application for access to numbering resources if the Bureau determines that the application requires further analysis to determine whether grating the application services the public interest), 63.04 (stating that applications for domestic section 214 transfer of control must show how the application is consistent with the public interest, convenience and necessity), 63.18 (stating that applications for domestic and international 214 authorizations must demonstrate how a grant of the applications will serve the public interest, convenience, and necessity).

[248] *See Policy Regarding Character Qualifications in Broadcast Licensing*, Gen. Docket Nos. 81-500, 78-100, Report, Order and Policy Statement, 102 FCC 2d 1179 (1986) (stating that the Commission may determine whether the public interest would be served by granting a particular application in the broadcast, common carrier, wireless, and other services, and that it is especially "concerned with misconduct which violates . . . a Commission rule or policy.").

enforcement process, there may be grounds for termination of Commission authorizations.[249] Our established section 214 revocation process described above satisfies due process requirements,[250] and we intend to apply it to all entities that we find to be continually violating our robocall mitigation rules.

71. *Future Review of Entities, Individual Company Owners, Directors, Officers, and Principals Applying for Commission Authorizations, Licenses, or Certifications*. Once we have revoked the section 214 or other Commission authorization, license, or certification of an entity that has engaged in continued violations of our robocall mitigation rules, we will consider the public interest impact of granting other future Commission authorizations, licenses, or certifications to the entity that was subject to the revocation, as well as individual company owners, directors, officers, and principals (either individuals or entities) of such entities.[251] We will consider the public interest impact as part of our established review processes for Commission applications at the time that they are filed. For example, a principal of a provider that had its section 214 authority revoked or that was removed from the Robocall Mitigation Database as a result of an enforcement action may be subject to a denial of other Commission authorizations, licenses, or certifications, including for international section 214 authority, or for approval to acquire an entity that holds blanket domestic section 214 authority or international section 214 authority. This is consistent with our current process in which we review many public interest factors in determining whether to grant an application, including whether an applicant for a license has the requisite citizenship, character, financial, technical, and other qualifications.[252] To ensure that we can accurately identify individual company owners, directors, officers, and principals of an entity for which we revoked authority, we intend to rely on information contained in providers' registrations filed in the Robocall Mitigation Database. Where that information is insufficient for this purpose, we will require entities undergoing revocation proceedings to identify their individual company owners, directors, officers, and principals as part of the revocation process.

72. We proposed in the *Fifth Caller ID Authentication Further Notice* that principals and others associated with entities subject to revocation would be banned from holding a 5% or greater ownership interest in "any entity that applies for or already holds any FCC license or instrument of authorization for the provision of a regulated service subject to Title II of the Act or of any entity otherwise engaged in the provision of voice service for a period of time to be determined."[253] No commenter addressed this proposal. The record contains no information on how we would undertake the complex process of identifying the providers or applicants that would be impacted by the 5% ownership trigger threshold, or whether we would risk negatively impacting the operations and customers of providers associated with the targeted principal, but which were not involved in the robocall offenses. Should we see an increased volume of repeat offenses of the robocall mitigation rules, we will consider whether to adopt rules permanently barring principals and others associated with entities subject to revocation from holding both existing and future Commission authorizations. Going forward now, we will generally consider whether it is in the public interest for individual company owners, directors, officers, and principals associated with an entity for which we have revoked a Commission authorization to obtain new Commission authorizations or licenses at the time that they, or an entity with which they

[249] VON Comments at 7.

[250] *See China Telecom Order on Revocation* at 15983-87, paras. 23-32.

[251] We expect that owners, directors, officers, and principals, whether or not they have control of the entity, have influence, management, or supervisory responsibilities for the entity subject to the revocation. *See* 47 CFR § 63.24(d), Note 1 (describing factors that could indicate influence or control such as authority to appoint executives for day-to-day operations, authority to make management decisions, or pay financial obligations).

[252] *See, e.g.*, *Applications of T-Mobile US, Inc., and Sprint Corporation, Consent to Transfer Control of Licenses and Authorizations*, WT Docket No. 18-197, Memorandum Opinion and Order, Declaratory Ruling, and Order of Proposed Modification, 34 FCC Rcd 10578, 10596-97, para. 43 (2019).

[253] *Fifth Caller ID Authentication Further Notice* at 81, para. 211.

are affiliated, apply for them. This is consistent with our stated intent in the *Fifth Caller ID Authentication Further Notice* to consider the impact these principals and others may have on "future" significant association with entities regulated by the Commission.[254]

73. We conclude that these new enforcement tools, acting in tandem with our new requirement for providers to submit their related entities and principals in their robocall mitigation plans, will ensure that bad actor providers and their principals will face potentially serious consequences for their repeated violation of our robocall mitigation rules.[255] These potential consequences reach beyond a forfeiture and appropriately subject these entities and principals to specified consequences and a thorough public interest review as required. We make clear that revoking a Commission authorization or license does not transform entities that have not been classified as common carriers into common carriers or extend our general jurisdiction over foreign providers.[256] Rather, this consequence merely allows the Commission discretion to revoke a Commission authorization or license that a provider, person, or entity would otherwise be eligible for or to deny an application for a Commission license or authorization by a principal of an entity subject to revocation. For this reason, we need not exempt foreign providers from this rule, as some commenters argue.[257]

5. Other Enforcement Matters

74. We decline to adopt a number of other enforcement proposals filed in the record. We do not adopt EPIC/NCLC's proposal to base enforcement actions, including removal from the Robocall Mitigation Database, solely on the number of tracebacks a provider receives.[258] We agree with commenters that while receiving a high number of traceback requests may be evidence of malfeasance in certain instances,[259] this is not always the case.[260] As CCA notes, "multiple traceback efforts . . . may simply reflect that the provider is a traffic aggregator serving numerous providers."[261] Our rules

[254] *Id.* at 79, para. 207.

[255] *See* EPIC/NCLC Comments at 16 (arguing for enforcement actions against "any provider who is affiliated with individuals or providers that have been previously subject to Commission action.").

[256] VON Comments at 7 ("[T]he Commission should proceed cautiously [in] suggesting that filing in the RMD extends" a section 214 operating authority to a foreign provider"); INCOMPAS Reply at 5 ("INCOMPAS is concerned that the Commission's proposal to find that non-common carrier providers registered in the RMD 'hold a Commission certification such that they are subject to the Commission's jurisdiction' may have unintended consequences that impact the effectiveness of the RMD.").

[257] *See* CCA Comments (urging that the Commission specifically exempt foreign providers from this rule and that failure to do so would discourage them from filing); INCOMPAS Reply at 5 (same).

[258] EPIC/NCLC Comments at 19 (proposing that "high-risk" providers be subject to expedited Robocall Mitigation Database suspension "after receiving a third traceback request within a 12-month period").

[259] In enforcement actions, the Commission has considered a high volume of tracebacks as a factor in determining whether a provider engaged in egregious and intentional misconduct. *See Spiller Forfeiture Order*, 36 FCC Rcd at 6257-58, paras. 60-63.

[260] *See* ITG Sept 1 *Ex Parte* at 6 (explaining that "raw traceback data can be both misleading and harmful. Absent proper context and appropriate investigation, raw traceback data can understate the complicity of purposefully evasive bad actors while at the same time incorrectly stating or overstating the responsibility of a voice service provider, including lesser-known small providers."); *see also* CCA Reply at 5-6; USTelecom Reply at 3 (opposing EPIC/NCLC's proposed "three strikes" traceback rule); Verizon Reply at 3 (arguing that basing liability on the number of tracebacks would "embrace unsupported presumptions about service provider culpability"); VON Reply at 3.

[261] CCA Comments at 12; *see also* VON Reply at 3 (arguing that there is no "rational basis" for Robocall Mitigation Database removal after three traceback requests within 12 months, but "[t]he critical issues are whether the voice service provider cooperated with the Industry Traceback Group and whether it's complying with its illegal robocall mitigation obligations."); INCOMPAS Reply at 3-4.

independently require providers to commit to respond to traceback requests—and to actually respond to such requests—in a certain time period, and they may be subject to forfeiture or removal for failure to do so.[262] We also decline to adopt licensing or bonding requirements for certain VoIP providers as EPIC/NCLC proposes.[263] As we have explained, we do not believe that separate robocall rules or obligations are appropriate for VoIP providers,[264] and EPIC/NCLC has not explained how to readily administer such a requirement,[265] or whether our current or proposed direct access requirements for VoIP providers address the same concerns.[266]

75. We decline to adopt EPIC/NCLC's strict liability standard for forfeiture or removal from the Robocall Mitigation Database for failure to block any illegal calls regardless of the circumstances, or their suggestion of an "interim" standard of assessing liability for transmitting illegal robocall traffic based on whether a provider "knew or should have known that [a] call was illegal."[267] Most parties opposed strict liability, and we again conclude that expectations to stop all illegal calls are not realistic and that a strict liability standard could lead to significant market disruptions.[268] EPIC/NCLC has not adequately explained why we should take a different approach now or why its proposed standards are consistent with the Act and our rules.[269] Similarly, we decline to adopt NCTA or ACA Connect's proposed "good faith"[270] or CCA's proposed "reasonableness" standards.[271]

---

[262] *See e.g.*, 47 CFR §§ 64.6305(a)(2) (requiring voice service providers to commit to respond to traceback requests "fully and timely"); 64.1200(n)(ii) (requiring gateway providers to respond to traceback requests within 24 hours).

[263] EPIC/NCLC Comments at 30.

[264] *See supra* para. 34.

[265] *See* VON Reply at 2-3 ("There are multiple problems with the Epic proposals. Most glaringly, there is no definition of 'non-facilities-based' VoIP providers, leaving to conjecture which providers the new application, licensing and bonding requirements would apply . . . also, how will the Commission determine the 'degree of risk associated with the applicant.'").

[266] *See e.g.*, *Direct Access Further Notice*, 36 FCC Rcd at 12910-21, paras. 6-29 (seeking comment on additional requirements for VoIP provider applications for direct access to numbers).

[267] EPIC/NCLC Comments at 10-12 (arguing that, among other things, a provider has duty to implement call analytics to "know" whether it is transmitting illegal robocalls and its failure to either do so or block any illegal calls from a particular source would result in liability).

[268] INCOMPAS Comments at 13-14; CCA Reply at 4 ("A strict liability standard would have extremely negative consequences for enterprises that lawfully send higher volume traffic, increasing their costs, while reducing competitive options."); VON Reply at 3; *Gateway Provider Order* at 42, para. 99 ("We therefore reiterate that, as with our prior rule [for voice service providers], we do not expect perfection [from gateway providers].").

[269] 47 U.S.C. §§ 312, 501-503; 47 CFR § 1.80(a); *see also* 47 U.S.C. § 312(f)(1) ("[T]he term "willful," when used with reference to the commission or omission of any act, means the conscious and deliberate commission or omission of such act, irrespective of any intent to violate any provision of this Act or any rule or regulation of the Commission authorized by this Act or by a treaty ratified by the United States.").

[270] NCTA Comments at 4 ("NCTA encourages the Commission to ensure that the proposal to impose forfeitures for failures to block calls after Commission notice on a per-call basis does not ensnare providers acting in good faith."); ACA Connects Reply at 3 (agreeing with NCTA's proposal and arguing that "[p]roviders making a good-faith effort to comply with any Commission call blocking requests—especially smaller providers or other providers receiving such a request for the first time—should not be subject to major penalties in the event that some illicit calls inadvertently make it through").

[271] CCA Comments at 9 ("Whether and when to hold a provider liable for passing illegal calls should be based on a reasonableness standard that incorporates factors such as the adequacy of, and compliance with, a mitigation plan and a history of responsiveness to traceback requests and actions taken after notice of illegal traffic."). EPIC/NCLC also proposes that we make tracebacks public. We do not consider this proposal in this item. *See* EPIC/NCLC Comments at 31-33.

D. STIR/SHAKEN Obligations of Satellite Providers

76. We conclude that satellite providers that do not use NANP numbers to originate calls or only use such numbers to forward calls to non-NANP numbers are not "voice service providers" under the TRACED Act and therefore do not have a STIR/SHAKEN implementation obligation. We also provide an ongoing extension from TRACED Act obligations to satellite providers that are small voice service providers and use NANP numbers to originate calls on the basis of a finding of undue hardship.[272]

77. The Commission previously provided small voice services providers, including satellite providers, an extension from STIR/SHAKEN implementation until June 30, 2023.[273] When the Wireline Competition Bureau reevaluated this extension in 2021, it declined to grant a request from the Satellite Industry Association (SIA) for an indefinite extension for satellite providers and stated that it would seek further comment on SIA's request before the June 30, 2023 extension expires.[274] In the *Fifth Caller ID Authentication Further Notice*, we sought comment on whether the TRACED Act requirements apply to some or all satellite providers and, if so, whether we should grant certain satellite providers a STIR/SHAKEN extension.[275] In addition to the questions raised in the *Fifth Caller ID Authentication Further Notice*, the Wireline Competition Bureau in August 2022 sought comment on the small provider extension generally and its applicability to satellite providers.[276] While several parties filed comments on the applicability of the TRACED Act and extensions to satellite providers in response to the *Fifth Caller ID Authentication Further Notice*,[277] no party filed comments on these issues in response to the *August 2022 Notice*. Therefore, the Wireline Competition Bureau deferred consideration of an extension for

[272] We note that in its earlier request, the Satellite Industry Association (SIA) sought relief for all small voice service satellite providers, noting that their "use of NANP resources is extremely limited." Satellite Industry Association Comments, WC Docket Nos. 20-68, 17-97, at 4 (filed Nov. 12, 2021) (SIA Nov. 2021 Comments). In their comments in response to the *Fifth Further Notice of Proposed Rulemaking*, SIA sought relief for "non-NANP" small voice service satellite providers, even in "de minimis" instances where calls are originated with NANP numbers. SIA Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 8 (filed Aug. 17, 2022) (SIA Comments). Because SIA's earlier and later justifications for relief largely overlap and because SIA does not provide an administrable way to distinguish "non-NANP" satellite providers that use NANP numbers infrequently from other satellite providers that use them more frequently, we grant relief to all small voice service satellite providers. However, as explained, the legal basis for that relief differs depending on whether a call is originated with a NANP number or not in a particular instance.

[273] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1877, paras. 40-42.

[274] *Wireline Competition Bureau Reevaluates STIR/SHAKEN Extensions Pursuant to Section 4(b)(5) of the TRACED Act*, WC Docket No. 17-97, Public Notice, 36 FCC Rcd 17748, 17750 (WCB 2021) (*WCB Dec. 2021 STIR/SHAKEN Extension Reevaluation Public Notice*).

[275] *Fifth Caller ID Authentication Further Notice* at 83-84, paras. 216-17. *See WCB Dec. 2021 STIR/SHAKEN Extension Reevaluation Public Notice,* 36 FCC Rcd at 17750. The TRACED Act requires that the Commission, 12 months after the date of the TRACED Act's enactment, and thereafter "as appropriate," assess burdens or barriers to implementation of STIR/SHAKEN. *See* 47 U.S.C. § 227b(b)(5)(A)(i). The TRACED Act further provides the Commission discretion to extend compliance with the implementation mandate "upon a public finding of undue hardship." *Id*. § 227b(b)(5)(A)(ii). Not less than annually thereafter, the Commission must consider revising or extending any delay of compliance previously granted and issue a public notice regarding whether such delay of compliance remains necessary. *Id*. § 227b(b)(5)(F). The Commission directed the Wireline Competition Bureau to make these annual assessments and to reevaluate the Commission's granted extensions and revise or extend them as necessary. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1896, para. 71.

[276] *See Wireline Competition Bureau Seeks Comment on Two Periodic TRACED Act Obligations Regarding Caller ID Authentication*, WC Docket No. 17-97, Public Notice, DA 22-831, at 3-4 (WCB Aug. 5, 2022) (*August 2022 Notice*).

[277] *See, e.g.*, SIA Comments; YouMail Comments at 5 & n.10; ZipDX Comments at 14-15; Satellite Industry Association Reply, CG Docket No. 17-59, WC Docket No. 17-97 (filed Sept. 16, 2022) (SIA Reply); ZipDX Reply at 7.

satellite providers and stated that the "arguments raised in . . . comments" in response to the *Fifth Caller ID Authentication Further Notice* "will be considered as part of that proceeding."[278]

78. *Satellite Providers Originating Calls Using Non-NANP Numbers*. We find that the record is sufficiently developed and now conclude that, where satellite providers originate calls using non-NANP numbers, they are not acting as "voice service providers" within the meaning of the TRACED Act. This conclusion is consistent with the TRACED Act's definition of voice service which requires that voice communications must use resources from the NANP.[279] We also agree with SIA that where satellite providers "utilize NANP resources for call forwarding to non-NANP numbers," such calls also fall outside of the definition of voice service.[280] This finding is consistent with the underlying purpose of the STIR/SHAKEN regime. One of the key aims of the TRACED Act, STIR/SHAKEN, and the Commission's implementing rules, is to prevent call spoofing.[281] Where a phone number is not displayed to the end user, as is the case in the satellite call forwarding scenario, call spoofing is not a concern.[282] SIA also argues that requiring satellite providers that originate calls using non-NANP numbers to implement STIR/SHAKEN would be an "undue hardship."[283] We need not reach that question because such providers are not acting as voice service providers when they originate calls with non-NANP numbers.

79. *Satellite Providers Originating Calls Using NANP Numbers*. We next permit an indefinite extension of time for small voice providers that are satellite providers originating calls using NANP numbers. SIA explains that there are "de minimis instances where satellite [providers] may assign NANP resources to their subscribers for caller ID purposes."[284] While we find that, in these cases, satellite providers are acting as voice service providers, we believe it is also appropriate to provide an indefinite extension for STIR/SHAKEN implementation to these providers by applying the TRACED Act's "undue hardship" standard.

80. The TRACED Act directed the Commission to assess burdens or barriers to the implementation of STIR/SHAKEN,[285] and granted the Commission discretion to extend the implementation deadline for a "reasonable period of time" based upon a "public finding of undue hardship."[286] In considering whether the hardship is "undue" under the TRACED Act—as well as whether an extension is for a "reasonable period of time"—it is appropriate to balance the hardship of compliance due to the "the burdens and barriers to implementation" faced by a voice service provider or

[278] *See Wireline Competition Bureau Performs Required Evaluation Pursuant to Section 64.6304(f) of the Commission's Rules*, WC Docket No. 17-97, Public Notice, DA 22-1342, at 3, n.17 (WCB Dec. 16, 2022). The Commission has previously found that whether or not a provider is a voice service provider should be determined on a call-by-call basis. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1870, para. 23.

[279] *See* TRACED Act § 4(a)(2)(defining "voice service" as a service that "that furnishes voice communications to an end user using resources from the North American Numbering Plan").

[280] SIA Comments at 6.

[281] *Gateway Provider Order* at 5-6, para. 8.

[282] SIA Comments at 7 ("Since a NANP resource used exclusively for call forwarding purposes is not, and cannot be spoofed, such 'use' does not fall under the definition of 'voice service' contained in the TRACED Act and the Commission's implementing regulations.").

[283] SIA Comments at 9.

[284] *Id*. at 8.

[285] TRACED Act § 4(b)(5)(A).

[286] *Id*. at § 4(b)(5)(A)(ii).

class of voice service providers with the benefit to the public of implementing STIR/SHAKEN expeditiously.[287]

81. We conclude that an indefinite extension is appropriate under this standard for small voice providers that are satellite providers originating calls using NANP numbers. According to SIA, the number of satellite subscribers using NANP resources "is miniscule."[288] Both SIA and YouMail argue that there is little evidence that satellite providers or their users are responsible for illegal robocalls[289] and that satellite service costs make the high-volume calling necessary for robocallers uneconomical.[290] The balancing of the benefits and burdens, therefore, counsels against requiring such providers to implement STIR/SHAKEN. While ZipDX opposes SIA's proposed extension, it does not address the specific arguments raised by SIA and YouMail.[291]

82. We note that the Commission must annually reevaluate TRACED Act extensions granted, ensuring that the Commission will be able to act quickly to prevent any unforeseen abuses.[292] While we provide small voice service satellite providers an extension from STIR/SHAKEN implementation, we make clear that they must, like other voice service providers with an extension, submit a certification to the Robocall Mitigation Database pursuant to our existing rules and the new obligations we adopt in this Report and Order.

E. Differential Treatment of International Roaming Traffic

83. We next decline to adopt rules in this Report and Order concerning the differential treatment of international roaming traffic.[293] In the *Fifth Caller ID Authentication Further Notice*, we sought comment on stakeholders' assertions that international cellular roaming traffic involving NANP numbers (i.e., traffic originated abroad from U.S. mobile subscribers carrying U.S. NANP numbers and terminated in the U.S.) is unlikely to carry illegal robocalls and therefore should be treated with a "lighter" regulatory touch.[294] As part of that inquiry, we also asked whether any separate regulatory regime for such traffic could be "gamed" by illegal robocallers by disguising their traffic as cellular roaming traffic.[295]

84. The record on this proposal is limited, and commenters addressing this issue disagree as to whether differential treatment of international roaming traffic is appropriate. CCA argues that a lighter

[287] *Small Provider Order*, 36 FCC Rcd at 17857, para. 35.

[288] SIA Comments at 8.

[289] *Id*. at 15-17; YouMail Comments at 5, n.10.

[290] SIA Comments at 16 ("The inherent design and functioning of satellite voice service makes it an immensely economically inhospitable platform for use by illegal robocallers.").

[291] ZipDX Comments at 14-15 (arguing that satellite providers can readily adopt hosted STIR/SHAKEN solutions and arguing against an indefinite extension); ZipDX Reply at 7 (arguing that non-NANP providers could get a waiver from STIR/SHAKEN obligations). As we explain, when a satellite provider transmits a call without NANP number, it is not acting as a voice service provider with a STIR/SHAKEN obligation.

[292] TRACED Act § 4(b)(5)(F)(i); YouMail Comments at 5, n.10 ("YouMail does not believe that STIR/SHAKEN requirements should be extended to satellite providers at this time because there is no evidence of significant satellite use for robocalls. However, the Commission should monitor this situation and act quickly if that fact changes.").

[293] We also decline to adopt rules concerning differential treatment of non-conversational traffic in this Report and Order. We continue to consider the record on this issue. *See Fifth Caller ID Authentication Further Notice* at 70-71, paras. 184-86; ZipDX Comments at 8-10.

[294] *See Fifth Caller ID Authentication Further Notice* at 89, para. 225.

[295] *See id*.

treatment is appropriate because such traffic does not generally carry robocalls,[296] and that it should be exempted from authentication requirements and the prohibition on accepting calls carrying U.S. NANP numbers sent directly from foreign providers not in the Robocall Mitigation Database.[297] Other commenters oppose treating this traffic differently.[298]

85. Given the limited record on this issue, particularly with respect to whether and how providers could readily identify or segregate such traffic for differential treatment, we direct the Wireline Competition Bureau to refer the issue to NANC for further investigation.

F. Summary of Cost Benefit Analysis

86. We find that the benefits of the rules we adopt today will greatly outweigh the costs imposed on providers. As we explained in the *First Caller ID Authentication Report and Order*, we concluded that our STIR/SHAKEN rules are likely to result in, at a minimum, $13.5 billion in annual benefits.[299] In the *Fifth Caller ID Authentication Further Notice*, we sought comment on our belief that our proposed rules and actions "would achieve a large share of the annual $13.5 billion benefit" and that the benefits "will far exceed the costs imposed on providers."[300] After reviewing the record in this proceeding, we confirm this conclusion.

87. Limiting the ability of illegal robocallers to evade existing rules will preserve and extend the benefits of STIR/SHAKEN. The new enforcement tools we adopt, as well as expanded call authentication and robocall mitigation obligations, will increase the effectiveness of our authentication regime, thereby allowing more illegal robocalls to be readily identified and stopped. As we found previously, we again conclude that an overall reduction in illegal robocalls from new rules will lower network costs by eliminating both unwanted traffic congestion and the labor costs of handling numerous customer complaints. This reduction in robocalls will also help restore confidence in the U.S. telephone network and facilitate reliable access to emergency and healthcare services.[301]

88. While several providers argue that a broad intermediate provider authentication obligation would impose significant costs without a material benefit,[302] in this Report and Order we adopt a more targeted obligation applicable to the first intermediate provider in the call path.[303] As we explained, by limiting the authentication obligation to the intermediate provider at the beginning of the

[296] CCA Comments at 14.

[297] *Id*. at 13-14. According to CCA, these exceptions should only apply where "the U.S. provider can definitively identify the traffic as roaming traffic, for example, where [it] utilizes segregated trunks." *Id*. at 14.

[298] Telnyx Comments at 4; ZipDX Comments at 16-17.

[299] *See First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3252, para. 25 (estimating that the benefits of eliminating the wasted time and nuisances caused by illegal scam robocalls will exceed $3 billion annually, and expecting "STIR/SHAKEN paired with call analytics to serve as a tool to effectively protect American consumers from fraudulent robocalls schemes that cost Americans approximately $10 billion annually").

[300] *See Fifth Caller ID Authentication Further Notice* at 63, para. 159.

[301] *See Gateway Provider Order* at 46-7, paras. 109, 111; *see also Spiller NAL*, 35 FCC Rcd at 5961, para. 33 ("Spoofed robocalls harm carriers by (1) burdening the carriers' networks with illegal calls, and (2) inducing enraged recipients of the illegal robocalls to complain, thereby adding to the workload of customer service agents, decreasing the perceived value of the service, and increasing carrier costs.").

[302] *See, e.g.*, CCA Comments at 1-2 (arguing that "further extending the authentication requirement to all intermediate providers will not materially reduce illegal robocalls"); Telnyx LLC Comments at 1-2; USTelecom Comments at 11-12; Verizon Reply at 6-8.

[303] *See supra* Section III.A.

call chain, we maximize the benefits of our requirement while minimizing its costs.[304] Indeed, intermediate providers can avoid any authentication burden if they require their upstream providers to only send them authenticated traffic.[305]

89. We acknowledge that the revised and expanded mitigation and Robocall Mitigation Database filing obligations we adopt today will impose limited short-term implementation costs.[306] Nevertheless, we conclude that the benefits of bringing all providers within the mitigation and Robocall Mitigation Database regime will produce significant benefits to the Commission and the public by increasing transparency and accountability, and by facilitating the enforcement of our rules.[307]

G. Legal Authority

90. Consistent with our proposals, we adopt the foregoing obligations pursuant to the legal authority we relied on in prior caller ID authentication and call blocking orders. We note that no commenter questioned our proposed legal authority to adopt these rules.

91. *Caller ID Authentication.* We conclude that the same authority through which we imposed caller ID authentication obligations on gateway providers—a subset of intermediate providers—applies equally to our rules that impose caller ID authentication obligations on non-gateway intermediate providers.[308] Specifically, we find authority to impose caller ID authentication obligations on the first intermediate providers in the call chain under section 251(e) of the Act and the Truth in Caller ID Act.[309] In the *Second Caller ID Authentication Report and Order*, the Commission found it had the authority to impose caller ID authentication obligations on intermediate providers under these provisions.[310] It reasoned that "[c]alls that transit the networks of intermediate providers with illegally spoofed caller ID are exploiting numbering resources" and so found authority under section 251(e).[311] The Commission found "additional, independent authority under the Truth in Caller ID Act" on the basis that such rules were necessary to "prevent . . . unlawful acts and to protect voice service subscribers from scammers and bad actors," stressing that intermediate providers "play an integral role in the success of STIR/SHAKEN across the voice network."[312] The Commission relied on this reasoning in adopting authentication obligations on gateway providers[313] and we therefore rely on this same legal authority to impose an authentication obligation on the first intermediate providers in the call chain.

92. *Robocall Mitigation.* We adopt our robocall mitigation provisions for non-gateway intermediate providers and voice service providers, including those without the facilities necessary to implement STIR/SHAKEN, pursuant to sections 201(b), 202(a), and 251(e) of the Communications Act; the Truth in Caller ID Act; and our ancillary authority, consistent with the authority we invoked to adopt analogous rules in the *Gateway Provider Order* and *Second Caller ID Authentication Report and*

[304] *See supra id*.

[305] *See supra* para. 20.

[306] *See supra* Section III.B.

[307] *See supra* Section III.A, B.

[308] *Gateway Provider Order* at 12-13, 47-48, paras. 25-27, 113 (defining "gateway providers" as a subset of intermediate providers).

[309] *See* 47 U.S.C. §§ 227(e), 251(e).

[310] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1931-32, paras. 153-55.

[311] *Id.* at 1931, para. 153.

[312] *Id.* at 1931, para. 154 (quoting *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3262, para. 44).

[313] *See Gateway Provider Order* at 47-48, para. 113.

Order.[314] We conclude that section 251(e) of the Act and the Truth in Caller ID Act authorize us to prohibit domestic intermediate providers and voice service providers from accepting traffic from non-gateway intermediate providers that have not filed in the Robocall Mitigation Database. In the *Second Caller ID Authentication Report and Order*, the Commission concluded that "section 251(e) gives us authority to prohibit intermediate providers and voice service providers from accepting traffic from both domestic and foreign voice service providers that do not appear in [the Robocall Mitigation Database]," noting that its "exclusive jurisdiction over numbering policy provides authority to take action to prevent the fraudulent abuse of NANP resources."[315] The Commission observed that "[i]llegally spoofed calls exploit numbering resources whenever they transit any portion of the voice network—including the networks of intermediate providers" and that "preventing such calls from entering an intermediate provider's or terminating voice service provider's network is designed to protect consumers from illegally spoofed calls."[316] The Commission found that the Truth in Caller ID Act provided additional authority for our actions to protect voice service subscribers from illegally spoofed calls.[317]

93. The Commission concluded that it had the authority to adopt these requirements pursuant to sections 201(b), 202(a), and 251(e) of the Act, as well as the Truth in Caller ID Act, and its ancillary authority.[318] Sections 201(b) and 202(a) provide the Commission with "broad authority to adopt rules governing just and reasonable practices of common carriers."[319] Accordingly, the Commission found that the new blocking rules were "clearly within the scope of our section 201(b) and 202(a) authority" and "that it is essential that the rules apply to all voice service providers," applying its ancillary authority in section 4(i).[320] The Commission also found that section 251(e) and the Truth in Caller ID Act provided the basis "to prescribe rules to prevent the unlawful spoofing of caller ID and abuse of NANP resources by all voice service providers,"[321] a category that includes VoIP providers and, in the context of our call blocking orders, intermediate providers.[322] We conclude that the same authority provides a basis to adopt the mitigation obligations we adopt in this Report and Order to the extent that providers are acting as common carriers.

94. While we conclude that our direct sources of authority provide an ample basis to adopt our proposed rules on all providers, our ancillary authority in section 4(i)[323] provides an independent basis to do so with respect to providers that have not been classified as common carriers. The Commission

[314] *See id.* at 48-49, paras. 114-19; *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1909-10, paras. 97-100. We sought comment on whether we should impose a mitigation duty on voice providers without the facilities necessary to implement STIR/SHAKEN on the basis of an ongoing extension from the TRACED Act. *See Fifth Caller ID Authentication Further Notice* at 82, para. 214. We conclude that because such providers were not granted an initial extension as a class under the TRACED Act, the clearest basis of authority for imposing a mitigation obligation is found in sections 201(b), 202(a), and 251(e) of the Communications Act; the Truth in Caller ID Act; and our ancillary authority.

[315] *Gateway Provider Order* at 48, para. 115; (quoting *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1910, para. 99).

[316] *Id*. (quoting *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1910, para. 115).

[317] *Id*. (citing *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1910, para. 100).

[318] *Id*. at 48-49, para. 117 (citing *Fourth Call Blocking Order*, 35 FCC at 15233-34, paras. 37-38).

[319] *Id*. at 49, para. 117 (quoting *Fourth Call Blocking Order*, 35 FCC Rcd at 15233, para. 37).

[320] *Id*. at 49, para. 117 (quoting *Fourth Call Blocking Order*, 35 FCC Rcd at 15233-34, para. 37); *see also* 47 U.S.C. § 154(i).

[321] *Gateway Provider Order* at 49, para 117 (quoting *Fourth Call Blocking Order*, 35 FCC Rcd at 15234, para. 37).

[322] *Id.* (*citing Fourth Call Blocking Order*, 35 FCC Rcd at 15222, n.2 (defining voice service providers to include intermediate providers for the purpose of the call blocking rules)).

[323] 47 U.S.C. § 154(i).

may exercise ancillary jurisdiction when two conditions are satisfied: (1) the Commission's general jurisdictional grant under Title I [of the Communications Act] covers the regulated subject; and (2) the regulations are reasonably ancillary to the Commission's effective performance of its statutorily mandated responsibilities.[324] We conclude that the regulations adopted in this Report and Order satisfy the first prong because providers that interconnect with the public switched telephone network and exchange IP traffic clearly offer "communication by wire and radio."[325]

95. With regard to the second prong, requiring providers to comply with our proposed rules is reasonably ancillary to the Commission's effective performance of its statutory responsibilities under sections 201(b), 202(a), and 251(e) of the Communications Act and the Truth in Caller ID Act as described above. With respect to sections 201(b) and 202(a), absent application of our proposed rules to providers that are not classified as common carriers, originators of robocalls could circumvent our proposed scheme by sending calls only via providers that have not yet been classified as common carriers.

96. *Enforcement*. We adopt our additional enforcement rules above pursuant to sections 501, 502, and 503 of the Act.[326] These provisions allow us to take enforcement action against common carriers as well as providers not classified as common carriers following a citation.[327] We rely on this same authority to revise section 1.80 of our rules by adding new maximum and base forfeiture amounts.[328]

IV. SIXTH FURTHER NOTICE OF PROPOSED RULEMAKING

A. Third-Party Caller ID Authentication

97. The Commission's rules require that a voice service provider "[a]uthenticate caller identification information for all SIP calls it originates and . . . to the extent technically feasible, transmit that call with authenticated caller identification information to the next voice service provider or intermediate provider in the call path."[329] In the *Fifth Caller ID Authentication Further Notice*, we sought comment on whether the Commission should amend its rules to address whether originating voice service providers may use third parties to perform their third-party authentication obligations.[330] The resulting record confirms that third-party authentication is occurring.[331] It does not, however, provide sufficient information to fully assess the impact that explicitly authorizing or prohibiting third-party authentication may have on the STIR/SHAKEN ecosystem. For instance, the record before us is not sufficient for us to understand the full scope of the various arrangements that exist between providers and third parties that authenticate their calls. Nor does it allow us to determine whether these third-party arrangements satisfy the requirements of the Commission's authentication rules, how and what information is shared within those arrangements, whether that information sharing implicates privacy, security, or other legal concerns, and whether they have a net positive or negative effect on the reliability of the STIR/SHAKEN framework and its objective to curtail illegal spoofing. We thus seek further comment on the use of third-party solutions to authenticate caller ID information and whether any changes should be made to the Commission's rules to permit, prohibit, or limit their use.

---

[324] *See*, *e.g.*, *Comcast Corp. v. FCC*, 600 F.3d 642, 646 (D.C. Cir. 2010); *American Library Ass'n v. FCC*, 406 F.3d 689 (D.C. Cir. 2005).

[325] 47 U.S.C. § 152(a).

[326] *Id*. §§ 501-503.

[327] *Id*. § 503(b)(5).

[328] 47 CFR § 1.80; *see also infra* Appx. A § 1.80 (adding maximum and minimum forfeiture amounts for per call violations of certain robocall rules).

[329] 47 CFR § 64.6301(a)(2).

[330] *See Fifth Caller ID Authentication Further Notice* at 87, para. 224.

[331] *See, e.g.*, Comcast Comments at 12; INCOMPAS Comments at 17; ZipDX Comments at 15-16; ACA Connects Reply at 2.

98. We start by seeking comment on the types of third-party authentication solutions being used by providers. Are originating or other providers entering into agreements with third parties to perform their authentication obligations under the Commission's rules and the ATIS technical standards? If so, who are these third parties, what is the nature of their relationship to the provider that has retained them, and how does any agreement between the provider and the third-party purport to assign responsibility for compliance with the Commission's authentication rules and the ATIS standards? We note that the ATIS technical standards acknowledge several scenarios in which providers may authenticate calls where they lack a direct relationship with the end user of a voice service.[332] These cases—including those involving providers serving enterprise, communications reseller, and value-added service provider customers[333]—generally involve an authenticating service provider that originates calls on behalf of a customer that itself maintains the direct relationship with the end user of the communications service.[334] Are third-party authentication arrangements limited to these types of situations or are providers outside of these limited scenarios contracting with third parties to perform all or part of their authentication responsibilities? For instance, are providers that originate calls themselves entering into arms-length agreements with third parties for authentication services? Are there third parties marketing caller ID authentication services for originating and other providers? We ask that commenters detail the different types of third-party authentication arrangements that are currently being employed by providers, address how prevalent each type of third-party authentication arrangement is in the STIR/SHAKEN ecosystem, and provide any available data substantiating how effective they are at facilitating the authentication of caller ID information.

99. Along those lines, we seek comment on whether, and under what circumstances, a third party may authenticate calls on behalf of a provider with A- or B-level attestations consistent with the ATIS standards. Pursuant to ATIS-1000074, in order to apply a B-level attestation for a call, the signing party must originate the call onto the IP-based service network and have a direct authenticated relationship with the customer.[335] An A-level attestation additionally requires the signing provider to establish a verified association with the telephone number used for the call.[336] Can a third-party authenticating a call on behalf of an originating provider satisfy all or any these criteria, and if so, how? Does the answer to that question depend on the nature of the relationship between the originating provider and the third party? For instance, is it possible for a third party that is a wholesale provider for a reseller,

[332] ATIS-1000088 at 10-11 ("[I]n a number of cases the end user is not the same entity as the 'customer,' so the customer identity is not directly tied to the end user. In these cases an end user identity is not needed for . . . authentication procedures . . . . As might be required in certain attestation scenarios, there may be a need for the [service provider] to establish (directly or indirectly through the customer) that the customer . . . is servicing a particular end user entity for [telephone number] authorization purposes."); *id*. at 5 (defining "customer" as "[t]ypically a service provider's subscriber, which may or not be the ultimate end-user of the telecommunications service," and which "may be a person, enterprise, reseller, or value added service provider;" and defining "end user" as "[t]he entity ultimately consuming the VoIP-based telecommunications service"); *see also* ATIS-1000074 at 12 (stating that, for full attestation, the "signing service provider is asserting that their customer can 'legitimately' use the [telephone number] that appears as the calling party (i.e., the Caller ID)" and that determining the "legitimacy of the [telephone numbers] the originator of the call can use is subject to signer-specific policy . . . .").

[333] ATIS-1000088 at 17-18.

[334] *Id*. at 13 ("In some . . . scenarios the [telephone number] assignments and/or authorizations apply to the indirect end user or call-initiation functions executed on behalf of the reseller's or [value-added service provider's] own customer. In those cases the [service provider's] customer should provide assurances that they can trace the identity of an indirect end user and that user's authorization to utilize a calling [telephone number]. The customer should be able to certify that only the authorized party (or calls originated on their behalf) will use the particular set of authorized [telephone numbers], and any traceback to the ultimate source will rely on the cooperation of the [service provider's] customer.").

[335] ATIS-1000074 at 12-13.

[336] *Id*. at 12.

or an intermediate provider, to apply A- or B-level attestations on behalf of an originating provider in a manner that complies with the ATIS attestation-level criteria, but not a different type of third party? Are there third parties authenticating calls on behalf of originating providers that can only apply C-level attestations under the ATIS criteria? If commenters contend that third parties can meet the ATIS criteria for signing calls with A- and B-level attestations because they effectively stand in the shoes of the originating provider with the direct relationship with the customer, we ask that they specify the legal bases for that conclusion, e.g., the specific grounds for an agency theory, if any, and/or how the terms of the ATIS standards may be construed to include the third-party arrangement.

100. To the extent commenters contend that third parties may satisfy the criteria to sign calls with A- or B-level attestations, what information must be shared between originating providers and third parties for those attestation levels to be applied, is that information sharing occurring, and does it implicate any legal or public interest concerns, including privacy concerns? For instance, does any of the information shared constitute customer proprietary network information?[337] Should any action taken by the Commission to explicitly authorize third-party authentication solutions be conditioned upon any particular restrictions or protections related to that information sharing? Should any explicit authorization of third-party authentication practices be conditioned upon providers ensuring that third parties have the information needed to apply A- or B-level attestations consistent with the ATIS standards?

101. We seek comment on whether there is a distinction between scenarios in which a third-party entity is retained to authenticate calls on behalf of a provider and the technical solutions described in the 2021 Small Providers Report produced by the NANC.[338] In that report, the NANC stated that small service providers may wish to "leverage [a] number of vendor solutions" offering third-party call signing services in order to comply with their STIR/SHAKEN implementation obligations under the Commission's rules,[339] identifying three options: (1)"hosted SHAKEN;"[340] (2) "carrier SHAKEN;"[341] and (3) "SHAKEN software."[342] Although each option involves different features, they each require the originating provider to "determin[e] the proper 'A' 'B,' or 'C' level attestation" for a given call and to use the third-party platform to sign the call using the originating provider's SPC token.[343] The NANC states that these options offer a cost-effective means for providers—particularly small providers—to implement STIR/SHAKEN consistent with the ATIS standards.[344] We seek comment on these technical solutions and the extent to which they are currently in use by providers. If commenters agree that they satisfy the criteria for signing calls under the ATIS standards, is that because the solutions require the originating provider to make the attestation level determinations and sign calls using the originating provider's SPC token, as opposed to arrangements in which a third party is allowed to make attestation level

[337] 47 U.S.C. § 222.

[338] North American Numbering Council, Call Authentication Trust Anchor Working Group, Deployment of STIR/SHAKEN by Small Voice Service Providers (Oct. 13, 2021) (NANC Small Providers Report), https://docs.fcc.gov/public/attachments/DOC-377426A1.pdf.

[339] NANC Small Providers Report at 6.

[340] *Id*. at 7 ("Hosted SHAKEN describes a turn-key SHAKEN authentication and verification solution offered in a public or private cloud that includes all the required SHAKEN components for offering a comprehensive standards-compliant solution . . . .").

[341] *Id*. at 7-8 ("Carrier SHAKEN describes another category of turn-key SHAKEN services offered by a growing number of Direct Inward Dialing (DID) or wholesale providers that also provide SIP termination to the PSTN. This service combines SHAKEN authentication service with SIP termination to the PSTN (transit service).").

[342] *Id*. at 8 ("SHAKEN Software is . . . a software-based SHAKEN solution deployed in-network by the [originating service provider] or [terminating service provider] in their respective data centers.").

[343] *Id*. at 7-8.

[344] *Id*. at 6-7.

determinations and sign calls using a different SPC token? Do these technical solutions, in fact, result in A- B-, and C-level attestations being accurately applied?

102. The record developed in response to the *Fifth Caller ID Authentication Further Notice* indicates that there could be benefits to explicitly authorizing third-party authentication arrangements. For instance, some commenters suggest that third-party authentication can strengthen the caller ID authentication regime by enabling STIR/SHAKEN to be applied to calls that would otherwise be transmitted without authentication.[345] We seek comment on the full range of benefits that could result from authorization of different third-party authentication arrangements. We also seek comment on the potential pitfalls of third-party authentication. For example, some commenters suggest that improper third-party signing practices are resulting in misleading and improper attestations, which in turn undermine the efficacy of the STIR/SHAKEN framework[346] and impair the analytics tools that rely on accurate attestation data to make blocking and labelling recommendations to their clients.[347]

103. Accordingly, we seek comment on whether the Commission should amend its rules to explicitly authorize third-party authentication and what, if any, limitations we should place on that authorization to ensure compliance with authentication requirements and the reliability of the STIR/SHAKEN framework. For instance, should we limit third-party authentication to scenarios akin to those described in the ATIS standards, where the entity authenticating the call is originating the call for a customer, such as a reseller or an enterprise customer? Notwithstanding the definitions provided by the ATIS standards,[348] should we "clarify that, for the purposes of the STIR/SHAKEN standard, a 'customer' means an end user and not a wholesale upstream provider" as USTelecom suggests?[349] Should we limit an authorization to the technical solutions described in the NANC's 2021 Small Providers Report? Alternatively, should we explicitly authorize third-party authentication more broadly but require the provider with the authentication obligation to make attestation-level determinations, rather than allowing them to rely on the third-party to make those determinations? If we were to explicitly authorize third-party authentication, should we also require third parties to sign calls using the provider's SPC token?[350] Should we prohibit providers from certifying to having implemented STIR/SHAKEN in the Robocall Mitigation Database unless their calls are signed with their own SPC token, whether directly or through a third party? Would such a requirement improve accountability by third-party authenticators? Is the

[345] *See* ACA Connects Comments at 4 ("[P]artnership with a wholesale provider has enabled many ACA Connects member companies to receive the benefits of STIR/SHAKEN *two years ahead* of the implementation deadline that applies to non-reseller providers of their size.") (emphasis in original); Comcast Comments at 12; CCA Comments at 12-13; INCOMPAS Comments at 17 ("For those that cannot maintain the framework natively, third party authentication has been a way for these providers to adequately meet the Commission's current requirements to transmit authenticated caller ID information to the next voice service provider."); RingCentral Comments at 10-11 (noting that "[t]hird-party authentication removes barriers to entry and enables integration of communications into a wide variety of services and applications");.

[346] TransNexus Comments at 4 (arguing that improper third-party signing practices "undermin[e] the accountability designed into the STIR/SHAKEN framework"); USTelecom Comments at 10 (arguing that improper third-party attestation practices "undermine the accountability the STIR/SHAKEN framework is intended to impose" and "water down the reliability of attestation levels"); ZipDX Comments at 16.

[347] Neustar *First Reevaluation of STIR/SHAKEN Extensions Public Notice* Comments at 4 (arguing that improper A-level attestations "mak[e] it more difficult for analytics tools to separate good calls from bad calls"); CTIA *First Reevaluation of STIR/SHAKEN Extensions Public Notice* Reply at 7; TNS, 2022 Robocall Investigation Report Ninth Ed. at 4 (Oct. 2022) (stating that inconsistent attestation practices make attestation data "less reliable as an analytical input") (TNS October Robocall Report).

[348] *See supra* n.335.

[349] USTelecom Comments at 11.

[350] *See, e.g.*, Comcast Comments at 12; TransNexus Comments at 1; USTelecom Comments at 10-11; ZipDX Comments at 16.

ability to obtain SPC tokens likely to present a barrier to providers' compliance with such a requirement? If so, in what circumstances? Are there security or other concerns implicated by a provider sharing its SPC token with another entity for the purpose of signing calls? Would that undermine trust in the STIR/SHAKEN regime?

104. We ask that commenters address the specific costs that would be incurred and gains that would be realized if we were to explicitly authorize or prohibit specific third-party authentication practices. Are there any other rules that the Commission would need to change if it were to explicitly authorize certain third-party authentication practices? What measures would the Commission need to implement to monitor compliance with the Commission's rules if third-party authentication arrangements are employed? For instance, should we amend our rules to explicitly require providers to identify any third-party solutions they rely upon in their Robocall Mitigation Database certifications and robocall mitigation plans, including the identity of the third party providing the solution, any requirements the provider has imposed on the third party to ensure compliance with the requirements of the ATIS technical standards and the Commission's rules, and what the provider itself does to ensure compliance with those requirements under the third-party arrangement? Are there any other compliance or enforcement measures that the Commission should adopt if it explicitly authorizes third-party authentication?

105. We also invite comment on whether a rulemaking is necessary to address third-party authentication or if another procedural device would be appropriate. For instance, to the extent commenters argue that third-party authentication is already authorized in the limited scenarios described in the ATIS standards, and no other third-party authentication arrangement should be permitted, should the Commission instead address these issues through a declaratory ruling? To the extent commenters advocate for imposing rules on third parties that authenticate calls on behalf of providers, rather than upon the providers themselves, we seek comment on the Commission's legal authority to do so.

106. Lastly, if the Commission were to explicitly authorize the use of third parties to authenticate caller ID information, we seek comment on whether we should require providers that are not currently required to implement STIR/SHAKEN because they do not have the facilities necessary to do so or are subject to an implementation extension to engage a third-party authentication solution for the SIP calls they originate. Would this significantly increase the number of calls authenticated with STIR/SHAKEN or is the impact likely to be minimal given the authentication obligation we adopt today for the first intermediate provider in the path of a SIP call and the fact that the implementation extension for facilities-based small providers will lapse on June 30, 2023?

B. Eliminating the Implementation Extension for Providers Unable to Obtain an SPC Token

107. We seek comment on whether to eliminate the STIR/SHAKEN implementation extension for providers that cannot obtain an SPC token. In the *Second Caller ID Authentication Report and Order*, the Commission granted voice service providers that are incapable of obtaining an SPC token due to Governance Authority policy a STIR/SHAKEN implementation extension until they are capable of obtaining said token.[351] The Wireline Competition Bureau recently found that "token access no longer stood as a significant barrier to full participation in STIR/SHAKEN," however, it retained the SPC token extension because "there may still be entities meeting the definition of a provider of 'voice service' that are unable to obtain a token, and thus unable to comply with the STIR/SHAKEN rules."[352]

108. We seek comment on whether the Commission should eliminate this extension. What are the benefits of, or drawbacks to, retaining the extension? Given changes in token access policy since the

[351] 47 CFR § 64.6304(b); *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1882-83, paras. 49-50. To participate in STIR/SHAKEN, a voice service provider must obtain an SPC token issued through the STIR/SHAKEN governance system.

[352] *Second Reevaluation of STIR/SHAKEN Extensions Public Notice* at 1.

Second Caller ID Authentication Report and Order making it easier to obtain an SPC token, which, if any, providers are likely to qualify for this extension today, and under what circumstances? Assuming some providers remain unable to obtain an SPC token, are there other ways the Commission could account for these providers in our rules, apart from an implementation extension? Alternatively, would the Commission's standard waiver provisions be sufficient protection for any providers unable to obtain an SPC token?[353] Are there other solutions that would allow any providers who remain unable to obtain an SPC token to participate in the STIR/SHAKEN framework? We seek comment on these and any alternative approaches to eliminating the SPC token extension.

C. Legal Authority

109. We propose to rely upon section 251(e) of the Act and the Truth in Caller ID Act to require providers to meet any such requirements we adopt.[354] We seek comment on this approach and whether there are any alternative sources of authority that we should consider.

110. We propose to rely on the TRACED Act to require originating providers to ensure that their calls are signed with their own token.[355] To eliminate the extension for token access, we propose to rely on our authority under the TRACED Act to revise any granted extensions.[356] We seek comment on these proposals. We also seek specific comment on our authority to eliminate an existing TRACED Act extension by Commission action outside of the annual extension reevaluation process mandated by the TRACED Act.[357] Are there any other sources of authority we should consider?

D. Digital Equity and Inclusion

111. The Commission, as part of its continuing effort to advance digital equity for all,[358] including people of color and others who have been historically underserved, marginalized, and adversely affected by persistent poverty and inequality, invites comment on any equity-related considerations[359] and benefits (if any) that may be associated with the proposals and issues discussed herein. Specifically, we seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility.

---

[353] 47 CFR § 1.3.

[354] *See* 47 U.S.C. §§ 227 (e), 251(e).

[355] TRACED Act § 4(b)(1) (requiring the Commission to adopt call authentication framework for voice service providers).

[356] *Id*. at § 4(b)(5)(F).

[357] *Id*. at § 4(b)(5)(F). The Wireline Competition Bureau recently completed such an assessment on delegated authority. *See Triennial STIR/SHAKEN Report*.

[358] Section 1 of the Communications Act of 1934 as amended provides that the FCC "regulat[es] interstate and foreign commerce in communication by wire and radio so as to make [such service] available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex." 47 U.S.C. § 151.

[359] We define the term "equity" consistent with Executive Order 13985 as the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment, such as Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality. *See* Exec. Order No. 13985, 86 Fed. Reg. 7009, Executive Order on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (Jan. 20, 2021).

V. PROCEDURAL MATTERS

112. *Final Regulatory Flexibility Analysis*. As required by the Regulatory Flexibility Act of 1980 (RFA),[360] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Fifth Caller ID Authentication Further Notice*.[361] The Commission sought written public comment on the possible significant economic impact on small entities regarding the proposals addressed in the *Fifth Caller ID Authentication Further Notice*, including comments on the IRFA.[362] Pursuant to the RFA, a Final Regulatory Flexibility Analysis (FRFA) is set forth in Appendix B. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of this *Sixth Report and Order*, including the FRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[363]

113. *Initial Regulatory Flexibility Analysis*. As required by the RFA, the Commission has prepared an IRFA of the possible significant economic impact on small entities of the policies and rules addressed in this *Sixth Further Notice*. The IRFA is set forth in Appendix C. Written public comments are requested on the IRFA. Comments must be filed by the deadlines for comments on the *Sixth Further Notice* indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of this *Sixth Further Notice*, including the IRFA, to the Chief Counsel for Advocacy of the SBA.[364]

114. *Paperwork Reduction Act*. This document may contain new and modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. Specifically, the rules adopted in 47 CFR §§ 64.6303(c), 65.6305(d), 65.6305(e) and 65.6305(f) may require new or modified information collections. This document will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other Federal agencies will be invited to comment on the new or modified information collection requirements contained in this proceeding.

115. The *Sixth Further Notice* also may contain proposed new and revised information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and OMB to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C § 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

116. *Congressional Review Act.* The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget (OMB), concurs, that this rule is "major" under the Congressional Review Act, 5 U.S.C. § 804(2). The Commission will send a copy of this Report and Order to Congress and the Government Accountability Office pursuant to 5 U.S.C. § 801(a)(1)(A).

117. *Ex Parte Presentations—Permit-But-Disclose.* The proceeding this *Sixth Further Notice* initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[365] Persons making *ex parte* presentations must file a copy of any written presentation or a

[360] *See* 5 U.S.C. § 603.

[361] *Fifth Caller ID Authentication Further Notice* at Appx. D.

[362] *Id.*

[363] *See* 5 U.S.C. § 603(a).

[364] *See id*.

[365] 47 CFR §§ 1.1200 *et seq.*

memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with section 1.1206(b) of the Commission's rules. In proceedings governed by section 1.49(f) of the Commission's rules or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.*, .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.[366]

118. *Comment Filing Procedures.* Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- Electronic Filers: Comments may be filed electronically using the Internet by accessing ECFS: https://www.fcc.gov/ecfs/.
- Currently, the Commission does not accept any hand-delivered or messenger-delivered filings as a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. In the event that the Commission announces the lifting of COVID-19 restrictions, a filing window will be opened at the Commission's office located at 9050 Junction Drive, Annapolis, Maryland 20701.[367]

119. Pursuant to section 1.49 of the Commission's rules, 47 CFR § 1.49, parties to this proceeding must file any documents in this proceeding using the Commission's Electronic Comment Filing System (ECFS): www.fcc.gov/ecfs.

120. *Accessible Formats*. To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice).

121. *Additional Information*. For further information about the *Further Notice*, contact Jonathan Lechter, Attorney Advisor, Competition Policy Division, Wireline Competition Bureau, at Jonathan.lechter@fcc.gov (202) 418-0984.

VI. ORDERING CLAUSES

122. Accordingly, pursuant to sections 4(i), 4(j), 201, 202, 214, 217, 227, 227b, 251(e), 303(r), 501, 502, and 503 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 154(j), 201, 202, 214, 217, 227, 227b, 251(e), 303(r), 501, 502, and 503, IT IS ORDERED that this *Sixth Report and Order* IS ADOPTED.

[366] 47 CFR § 1.49(f).

[367] *Amendment of the Commission's Rules of Practice and Procedure*, Order, 35 FCC Rcd 5450 (OMD 2020).

123. IT IS FURTHER ORDERED that, pursuant to sections 4(i), 4(j), 201, 202, 217, 227, 227b, 251(e), and 303(r) of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 154(j), 201, 202, 217, 227, 227b, 251(e), and 303(r), this *Sixth Further Notice of Proposed Rulemaking* IS ADOPTED.

124. IT IS FURTHER ORDERED that parts 0, 1, and 64 of the Commission's rules ARE AMENDED as set forth in Appendix A.

125. IT IS FURTHER ORDERED that, pursuant to sections 1.4(b)(1) and 1.103(a) of the Commission's rules, 47 CFR §§ 1.4(b)(1), 1.103(a), and this *Sixth Report and Order*, including the redesignation, renumbering, and addition of section designations as described in Appendix A, SHALL BE EFFECTIVE 60 days after publication in the Federal Register, except that: (1) the amendments to 47 CFR §§ 65.6303(c)(2), 65.6305(d), 65.6305(e) and 65.6305(f) as described in Appendix A will not be effective until OMB completes any review that the Wireline Competition Bureau determines is required under the Paperwork Reduction Act; and (2) amendments to 47 CFR § 65.6305(g) as described in Appendix A will not be effective until an effective date is announced by the Wireline Competition Bureau. The Commission directs the Wireline Competition Bureau to announce effective dates for 47 CFR §§ 64.6303(c)(2), 65.6305(d), 65.6305(e), 65.6305(f) and 65.6305(g) by subsequent Public Notice.

126. IT IS FURTHER ORDERED that the Office of the Managing Director, Performance Evaluation and Records Management, SHALL SEND a copy of this *Sixth Report and Order* in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, see 5 U.S.C. § 801(a)(1)(A).

127. IT IS FURTHER ORDERED that the Commission's Consumer & Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this *Sixth Report and Order*, including the Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

128. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this *Sixth Further Notice of Proposed Rulemaking*, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A

Final Rules

The Federal Communications Commission amends Parts 0, 1, and 64 of Title 47 of the Code of Federal Regulations as follows:

PART 0—COMMISSION ORGANIZATION

Subpart A—Organization

1. Amend section 0.111 by revising paragraph (a) to read as follows:

* * * * *

(28) Take enforcement action, including de-listing from the Robocall Mitigation Database, against any provider:

(i) Whose certification required by § 64.6305 is deficient after giving that provider notice and an opportunity to cure the deficiency; or

(ii) Who accepts calls directly from a provider not listed in the Robocall Mitigation Database in violation of § 64.6305(g).

(29) Take enforcement action, including revoking an existing section 214 authorization, license, or instrument for any entity that has repeatedly violated sections 64.6301, 64.6302, or 64.6305. The Commission or the Enforcement Bureau under delegated authority will provide prior notice of its intent to revoke an existing license or instrument of authorization and follow applicable revocation procedures, including providing the authorization holder with a written opportunity to demonstrate why revocation is not warranted.

PART 1—PRACTICE AND PROCEDURE

Subpart A—General Rules of Practice and Procedure

2. Amend section 1.80 by redesignating paragraphs (b)(9) as (b)(10), (b)(10) as (b)(11), and (b)(11) as (b)(12), adding new paragraph (b)(9), and revising paragraphs (b)(11) and (b)(12) to read as follows:

(9) ***Forfeiture penalty for a failure to block.*** Any person determined to have failed to block illegal robocalls pursuant to § 64.6305(g) and § 64.1200(n) of the Commission's rules shall be liable to the United States for a forfeiture penalty of no more than $23,727 for each violation, to be assessed on a per-call basis.

(10) ***Maximum forfeiture penalty for any case not previously covered.*** In any case not covered in paragraphs (b)(1) through (b)(9) of this section, the amount of any forfeiture penalty determined under this section shall not exceed $23,727 for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $177,951 for any single act or failure to act described in paragraph (a) of this section.

(11) * * *

Table 1 to Paragraph (b)(11) - Base Amounts for Section 503 Forfeitures

Forfeitures	Violation amount
Misrepresentation/lack of candor	(1)
Failure to file required DODC required forms, and/or filing materially inaccurate or incomplete DODC information	$15,000
Construction and/or operation without an instrument of authorization for the service	10,000
Failure to comply with prescribed lighting and/or marking	10,000
Violation of public file rules	10,000
Violation of political rules: Reasonable access, lowest unit charge, equal opportunity, and discrimination	9,000
Unauthorized substantial transfer of control	8,000
Violation of children's television commercialization or programming requirements	8,000
Violations of rules relating to distress and safety frequencies	8,000
False distress communications	8,000
EAS equipment not installed or operational	8,000
Alien ownership violation	8,000
Failure to permit inspection	7,000
Transmission of indecent/obscene materials	7,000
Interference	7,000
Importation or marketing of unauthorized equipment	7,000
Exceeding of authorized antenna height	5,000
Fraud by wire, radio or television	5,000
Unauthorized discontinuance of service	5,000
Use of unauthorized equipment	5,000
Exceeding power limits	4,000
Failure to Respond to Commission communications	4,000
Violation of sponsorship ID requirements	4,000
Unauthorized emissions	4,000
Using unauthorized frequency	4,000
Failure to engage in required frequency coordination	4,000
Construction or operation at unauthorized location	4,000
Violation of requirements pertaining to broadcasting of lotteries or contests	4,000
Violation of transmitter control and metering requirements	3,000

Failure to file required forms or information	3,000
Per call violations of the robocall blocking rules	2,500
Failure to make required measurements or conduct required monitoring	2,000
Failure to provide station ID	1,000
Unauthorized pro forma transfer of control	1,000
Failure to maintain required records	1,000

Table 2 to Paragraph (b)(11) - Violations Unique to the Service

* * * * *

Table 3 to Paragraph (b)(11) - Adjustment Criteria for Section 503 Forfeitures

* * * * *

Table 4 to Paragraph (b)(11) - Non-Section 503 Forfeitures That Are Affected by the Downward Adjustment Factors[1]

* * * * *

[1] Unlike section 503 of the Act, which establishes maximum forfeiture amounts, other sections of the Act, with two exceptions, state prescribed amounts of forfeitures for violations of the relevant section. These amounts are then subject to mitigation or remission under section 504 of the Act. One exception is section 223 of the Act, which provides a maximum forfeiture per day. For convenience, the Commission will treat this amount as if it were a prescribed base amount, subject to downward adjustments. The other exception is section 227(e) of the Act, which provides maximum forfeitures per violation, and for continuing violations. The Commission will apply the factors set forth in section 503(b)(2)(E) of the Act and this table 4 to determine the amount of the penalty to assess in any particular situation. The amounts in this table 4 are adjusted for inflation pursuant to the Debt Collection Improvement Act of 1996 (DCIA), 28 U.S.C. 2461. These non-section 503 forfeitures may be adjusted downward using the "Downward Adjustment Criteria" shown for section 503 forfeitures in table 3 to this paragraph (b)(11).

Note 2 to paragraph (b)(11): *Guidelines for Assessing Forfeitures.* The Commission and its staff may use the guidelines in tables 1 through 4 of this paragraph (b)(11) in particular cases. The Commission and its staff retain the discretion to issue a higher or lower forfeiture than provided in the guidelines, to issue no forfeiture at all, or to apply alternative or additional sanctions as permitted by the statute. The forfeiture ceilings per violation or per day for a continuing violation stated in section 503 of the Communications Act and the Commission's rules are described in paragraph (b)(12) of this section. These statutory maxima became effective September 13, 2013. Forfeitures issued under other sections of the Act are dealt with separately in table 4 to this paragraph (b)(11).

(12) ***Inflation adjustments to the maximum forfeiture amount.***

* * * * *

Table 5 to Paragraph (b)(12)(ii)

* * * * *

Note 3 to paragraph (b)(12): Pursuant to Public Law 104-134, the first inflation adjustment cannot exceed 10 percent of the statutory maximum amount.

PART 64—MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

Subpart HH—Caller ID Authentication

3. Amend section 64.6300 by redesignating paragraphs (h) as (i), (i) as (j), (j) as (k), (k) as (l), (l) as (m), and (m) as (n), (n) as (o) and adding new paragraph (h) to read as follows:

§ 64.6300 Definitions.

(h) ***Non-gateway intermediate provider.*** The term "non-gateway intermediate provider" means any entity that is an intermediate provider as that term is defined by paragraph (g) of this section that is not a gateway provider as that term is defined by paragraph (d) of this section.

4. Amend section 64.6302 by adding paragraph (d) to read as follows.

§ 64.6302 Caller ID authentication by intermediate providers.

* * * * *

(d) Notwithstanding paragraph (b) of this section, a non-gateway intermediate provider must, not later than December 31, 2023, authenticate caller identification information for all calls it receives directly from an originating provider and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call, unless that non-gateway intermediate provider is subject to an applicable extension in § 64.6304.

5. Amend section 63.6303 by adding paragraph (c) to read as follows.

§ 64.6303 Caller ID authentication in non-IP networks.

* * * * *

(c) Except as provided in § 64.6304, not later than December 31, 2023, a non-gateway intermediate provider receiving a call directly from an originating provider shall either:

(1) Upgrade its entire network to allow for the processing and carrying of SIP calls and fully implement the STIR/SHAKEN framework as required in § 64.6302(d) throughout its network; or

(2) Maintain and be ready to provide the Commission on request with documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non-internet Protocol caller identification authentication solution, or actively testing such a solution.

6. Amend section 64.6304 by revising paragraph (a), (b), and (d) to read as follows:

§ 64.6304 Extension of Implementation Deadline

(a) * * *

(1) * * *

(ii) A small voice service provider notified by the Enforcement Bureau pursuant to § 0.111(a)(27) of this chapter that fails to respond in a timely manner, fails to respond with the information requested by the Enforcement Bureau, including credible evidence that the robocall traffic identified in the notification is not illegal, fails to demonstrate that it taken steps to effectively mitigate the traffic, or if the Enforcement Bureau determines the provider violates § 64.1200(n)(2), will no longer be exempt from the requirements of § 64.6301 beginning 90 days following the date of the Enforcement Bureau's determination, unless the extension would otherwise terminate earlier pursuant to paragraph (a)(1) introductory text or (a)(1)(i), in which case the earlier deadline applies; and

(iii) Small voice service providers that originate calls via satellite using North American Numbering Plan numbers are deemed subject to a continuing extension of § 64.6301.

* * * * *

(b) ***Voice service providers, gateway providers, and non-gateway intermediate providers that cannot obtain an SPC token***. Voice service providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6301 until they are capable of obtaining an SPC token. Gateway providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6302(c) regarding call authentication. Non-gateway intermediate providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6302(d) regarding call authentication.

* * * * *

(d) ***Non-IP Networks.*** Those portions of a voice service provider, gateway provider, or non-gateway intermediate provider's network that rely on technology that cannot initiate, maintain, carry, process, and terminate SIP calls are deemed subject to a continuing extension. A voice service provider subject to the foregoing extension shall comply with the requirements of § 64.6303(a) as to the portion of its network subject to the extension, a gateway provider subject to the foregoing extension shall comply with the requirements of § 64.6303(b) as to the portion of its network subject to the extension, and a non-gateway intermediate provider receiving calls directly from an originating provider subject to the foregoing extension shall comply with the requirements of § 64.6303(c) as to the portion of its network subject to the extension.

* * * * *

7. Amend section 64.6305 by redesignating paragraph (c) as (d), (d) as (e) and (e) as (g), revising paragraphs (a), (b), (d), (e) and (g), and adding new paragraphs (c) and (f) to read as follows:

§ 64.6305 Robocall mitigation and certification.

(a) * * *

(1) Each voice service provider shall implement an appropriate robocall mitigation program.

* * * * *

(b) * * *

(1) Each gateway provider shall implement an appropriate robocall mitigation program.

* * * * *

(c) Robocall Mitigation program requirements for non-gateway intermediate providers.

(1) Each non-gateway intermediate provider shall implement an appropriate robocall mitigation program.

(2) Any robocall mitigation program implemented pursuant to paragraph (c)(1) of this section shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls.

(d) * * *

(1) A voice service provider shall certify that all of the calls that it originates on its network are subject to a robocall mitigation program consistent with paragraph (a), that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and to one of the following:

(i) It has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it originates are compliant with § 64.6301(a)(1) and (2);

(ii) It has implemented the STIR/SHAKEN authentication framework on a portion of its network and all calls it originates on that portion if its network are compliant with § 64.6301(a)(1); or

(iii) It has not implemented the STIR/SHAKEN authentication framework on any portion of its network.

(2) A voice service provider shall include the following information in its certification in English or with a certified English translation:

(i) Identification of the type of extension or extensions the voice service provider received under § 64.6304, if the voice service provider is not a foreign voice service provider, and the basis for that extension or extensions, or an explanation of why it is unable to implement STIR/SHAKEN due to a lack of control over the network infrastructure necessary to implement STIR/SHAKEN;

(ii) The specific reasonable steps the voice service provider has taken to avoid originating illegal robocall traffic as part of its robocall mitigation program, including a description of how it complies with its obligation to know its customers pursuant to § 64.1200(n)(3), any procedures in place to know its upstream providers, and the analytics system(s) it uses to identify and block illegal traffic, including whether it uses any third-party analytics vendor(s) and the name(s) of such vendor(s).

(iii) A statement of the voice service provider's commitment to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls; and

(iv) State whether, at any time in the prior two years, the filing entity (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description; and, if so (2) provide a description of any such action or investigation, including all law enforcement or regulatory agencies involved, the date that any action or investigation was commenced, the current status of the action or investigation, a summary of the findings

of wrongdoing made in connection with the action or investigation, and whether any final determinations have been issued.

(3) All certifications made pursuant to paragraph (d)(1) and (2) of this section shall:

(i) Be filed in the appropriate portal on the Commission's website; and

(ii) Be signed by an officer in conformity with 47 CFR 1.16.

(4) A voice service provider filing a certification shall submit the following information in the appropriate portal on the Commission's website:

(i) The voice service provider's business name(s) and primary address;

(ii) Other business names in use by the voice service provider;

(iii) All business names previously used by the voice service provider;

(iv) Whether the voice service provider is a foreign voice service provider;

(v) The name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues;

(vi) Whether the voice service provider is (1) a voice service provider with a STIR/SHAKEN implementation obligation directly serving end users; (2) a voice service provider with a STIR/SHAKEN implementation obligation acting as a wholesale provider originating calls on behalf of another provider or providers; or (3) a voice service provider without a STIR/SHAKEN implementation obligation; and

(vii) The voice service provider's OCN, if it has one.

(5) A voice service provider shall update its filings within 10 business days of any change to the information it must provide pursuant to paragraphs (d)(1) through (4) of this section.

* * * * *

(e) * * *

(1) A gateway provider shall certify that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with (b)(1) of this section, that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and to one of the following:

(i) * * * * *

(2) A gateway provider shall include the following information in its certification made pursuant to paragraph (e)(1), in English or with a certified English translation:

(i) Identification of the type of extension or extensions the gateway provider received under § 64.6304 and the basis for that extension or extensions, or an explanation of why it is unable to implement STIR/SHAKEN due to a lack of control over the network infrastructure necessary to implement STIR/SHAKEN;

(ii) The specific reasonable steps the gateway provider has taken to avoid carrying or processing illegal robocall traffic as part of its robocall mitigation program, including a description of how it complies with its obligation to know its upstream providers pursuant to § 64.1200(n)(4), the analytics system(s) it uses to identify and block illegal traffic, and whether it uses any third-party analytics vendor(s) and the name(s) of such vendor(s);

(iii) A statement of the gateway provider's commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls; and

(iv) State whether, at any time in the prior two years, the filing entity (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description; and, if so (2) provide a description of any such action or investigation, including all law enforcement or regulatory agencies involved, the date that any action or investigation was commenced, the current status of the action or investigation, a summary of the findings of wrongdoing made in connection with the action or investigation, and whether any final determinations have been issued.

(3) All certifications made pursuant to paragraph (e)(1) and (2) of this section shall:

(i) Be filed in the appropriate portal on the Commission's website; and

(ii) Be signed by an officer in conformity with 47 CFR 1.16.

(4) A gateway provider filing a certification shall submit the following information in the appropriate portal on the Commission's website:

(i) The gateway provider's business name(s) and primary address;

(ii) Other business names in use by the gateway provider;

(iii) All business names previously used by the gateway provider;

(iv) Whether the gateway provider or any affiliate is also foreign voice service provider;

(v) The name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues.

(vi) Whether the gateway provider is (1) a gateway provider with a STIR/SHAKEN implementation obligation; or (2) a gateway provider without a STIR/SHAKEN implementation obligation; and

(vii) The gateway provider's OCN, if it has one.

(5) A gateway provider shall update its filings within 10 business days to the information it must provide pursuant to paragraphs (e)(1) through (4) of this section, subject to the conditions set forth in (d)(5)(i) and (ii) of this section.

(f) Certification by non-gateway intermediate providers in the Robocall Mitigation Database.

(1) A non-gateway intermediate provider shall certify that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with paragraph (c), that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and to one of the following:

(i) It has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant with § 64.6302(b);

(ii) It has implemented the STIR/SHAKEN authentication framework on a portion of its network and calls it carries or processes on that portion of its network are compliant with § 64.6302(b); or

(iii) It has not implemented the STIR/SHAKEN authentication framework on any portion of its network for carrying or processing calls.

(2) A non-gateway intermediate provider shall include the following information in its certification made pursuant to paragraph (f)(1) in English or with a certified English translation:

(i) Identification of the type of extension or extensions the non-gateway intermediate provider received under § 64.6304, if the non-gateway intermediate provider is not a foreign provider, and the basis for that extension or extensions, or an explanation of why it is unable to implement STIR/SHAKEN due to a lack of control over the network infrastructure necessary to implement STIR/SHAKEN;

(ii) The specific reasonable steps the non-gateway intermediate provider has taken to avoid carrying or processing illegal robocall traffic as part of its robocall mitigation program, including a description of any procedures in place to know its upstream providers and the analytics system(s) it uses to identify and block illegal traffic, including whether it uses any third-party analytics vendor(s) and the name of such vendor(s);

(iii) A statement of the non-gateway intermediate provider's commitment to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls; and

(iv) State whether, at any time in the prior two years, the filing entity (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description; and, if so (2) provide a description of any such action or investigation, including all law enforcement or regulatory agencies involved, the date that any action or investigation was commenced, the current status of the action or investigation, a summary of the findings of wrongdoing made in connection with the action or investigation, and whether any final determinations have been issued.

(3) All certifications made pursuant to paragraph (f)(1) and (2) of this section shall:

(i) Be filed in the appropriate portal on the Commission's website; and

(ii) Be signed by an officer in conformity with 47 CFR 1.16.

(4) A non-gateway intermediate provider filing a certification shall submit the following information in the appropriate portal on the Commission's website:

(i) The non-gateway intermediate provider's business name(s) and primary address;

(ii) Other business names in use by the non-gateway intermediate provider;

(iii) All business names previously used by the non-gateway intermediate provider;

(iv) Whether the non-gateway intermediate provider or any affiliate is also foreign voice service provider;

(v) The name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues;

(vi) Whether the non-gateway intermediate provider is (1) a non-gateway intermediate provider with a STIR/SHAKEN implementation obligation; or (2) a non-gateway intermediate provider without a STIR/SHAKEN implementation obligation; and

(vii) The non-gateway intermediate service provider's OCN, if it has one.

(5) A non-gateway intermediate provider shall update its filings within 10 business days of any change to the information it must provide pursuant to paragraphs (f)(1) through (f)(5) subject to the conditions set forth in paragraphs (d)(5)(i) and (ii) of this section.

(g) * * *

* * * * *

(4) *Accepting traffic from non-gateway intermediate providers*. Intermediate providers and voice service providers shall accept calls directly from a non-gateway intermediate provider only if that non-gateway intermediate provider's filing appears in the Robocall Mitigation Database in accordance with paragraph (f) of this section, showing that the non-gateway intermediate provider affirmatively submitted the filing, and that filing has not been de-listed pursuant to an enforcement action.

(5) Public Safety Safeguards. Notwithstanding paragraphs (g)(1) through (4) of this section:

* * * * *

APPENDIX B

Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980 (RFA),[1] as amended, an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Further Notice of Proposed Rulemaking* adopted in May 2022 (*Fifth Caller ID Authentication Further Notice*).[2] The Commission sought written public comment on the proposals in the *Fifth Caller ID Authentication Further Notice*, including comment on the IRFA. The comments received are discussed below. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.[3]

A. Need for, and Objectives of, the Order

2. The *Sixth Report and Order* takes important steps in the fight against illegal robocalls by strengthening caller ID authentication obligations, expanding robocall mitigation rules, and granting an indefinite extension for small voice service providers that are also satellite providers originating calls using NANP numbers on the basis of undue hardship.[4] The decisions we make here protect consumers from unwanted and illegal calls while balancing the legitimate interests of callers placing lawful calls.

3. First, the *Sixth Report and Order* requires any non-gateway intermediate provider that receives an unauthenticated SIP call directly from an originating provider to authenticate the call.[5] Second, it requires non-gateway intermediate providers subject to the authentication obligation to comply with, at a minimum, the version of the standards in effect on December 31, 2023, along with any errata.[6] Third, it requires all providers—including intermediate providers and voice service providers without the facilities necessary to implement STIR/SHAKEN—to: (1) take "reasonable steps" to mitigate illegal robocall traffic; (2) submit a certification to the Robocall Mitigation Database regarding their STIR/SHAKEN implementation status along with other identifying information; and (3) submit a robocall mitigation plan to the Robocall Mitigation Database.[7] Fourth, it requires all providers to commit to fully respond to traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers that use its services to originate, carry, or process illegal robocalls.[8] Fifth, it requires downstream providers to block traffic received directly from non-gateway intermediate providers that have not submitted a certification in the Robocall Mitigation Database or have been removed through enforcement actions.[9] Finally, the *Sixth Report and Order* grants an ongoing STIR/SHAKEN implementation extension on the basis of undue hardship for satellite providers that are small service providers using NANP numbers to originate calls.[10]

---

[1] 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601-612, has been amended by the Contract With America Advancement Act of 1996, Public Law No. 104-121, 110 Stat. 847 (1996) (CWAAA). Title II of the CWAAA is the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA).

[2] *Fifth Caller ID Authentication Further Notice* at Appx. D.

[3] *See* 5 U.S.C. § 604.

[4] *See Sixth Report and Order* Section III.

[5] *Id.* Section III.A.1.

[6] *Id.* Section III.A.2-3.

[7] *Id.* Section III.B.1.

[8] *Id.* Section III.B.1.

[9] *Id.* Section III.B.2.

[10] *Id.* Section III.D.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

4. There were no comments raised that specifically addressed the proposed rules and policies presented in the Fifth Caller ID Authentication Further Notice IRFA.[11] Nonetheless, the Commission considered the potential impact of the rules proposed in the IRFA on small entities and took steps where appropriate and feasible to reduce the compliance burden for small entities in order to reduce the economic impact of the rules enacted herein on such entities.

C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration

5. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA), and to provide a detailed statement of any change made to the proposed rules as a result of those comments.[12] The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

D. Description and Estimate of the Number of Small Entities to Which Rules Will Apply

6. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the rules adopted herein.[13] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "mall governmental jurisdiction."[14] In addition, the term "small business" has the same meaning as the term "small-business concern" under the Small Business Act.[15] A "small-business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[16]

7. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein.[17] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[18] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 32.5 million businesses.[19]

---

[11] *Fifth Caller ID Authentication Further Notice* at 122-35, Appx. D.

[12] 5 U.S.C. § 604(a)(3).

[13] *See* 5 U.S.C. § 603(b)(3).

[14] *See* 5 U.S.C. § 601(6).

[15] *See* 5 U.S.C. § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[16] *See* 15 U.S.C. § 632.

[17] *See* 5 U.S.C. § 601(3)-(6).

[18] *See* SBA, Office of Advocacy, Frequently Asked Questions, "What is a small business?," https://cdn.advocacy.sba.gov/wp-content/uploads/2021/11/03093005/Small-Business-FAQ-2021.pdf. (Nov 2021).

[19] *Id.*

8. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[20] The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations.[21] Nationwide, for tax year 2020, there were approximately 447,689 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.[22]

9. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[23] U.S. Census Bureau data from the 2017 Census of Governments[24] indicate there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[25] Of this number there were 36,931 general purpose governments (county[26], municipal and town or township[27]) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts[28] with enrollment

[20] *See* 5 U.S.C. § 601(4).

[21] The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number small organizations in this small entity description. S*ee* Annual Electronic Filing Requirement for Small Exempt Organizations — Form 990-N (e-Postcard), "Who must file."

https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

[22] *See* Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO BMF data for businesses for the tax year 2020 with revenue less than or equal to $50,000, for Region 1-Northeast Area (58,577), Region 2-Mid-Atlantic and Great Lakes Areas (175,272), and Region 3-Gulf Coast and Pacific Coast Areas (213,840) that includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

[23] *See* 5 U.S.C. § 601(5).

[24] *See* 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* Census of Governments, https://www.census.gov/programs-surveys/cog/about.html.

[25] *See* U.S. Census Bureau, 2017 Census of Governments – Organization Table 2. Local Governments by Type and State: 2017 [CG1700ORG02], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). *See also* tbl.2. CG1700ORG02 Table Notes_Local Governments by Type and State_2017.

[26] *See id.* at tbl.5. County Governments by Population-Size Group and State: 2017 [CG1700ORG05], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

[27] *See id. at* tbl.6. Subcounty General-Purpose Governments by Population-Size Group and State: 2017 [CG1700ORG06], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 18,729 municipal and 16,097 town and township governments with populations less than 50,000.

[28] *See id.* at tbl.10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2017 [CG1700ORG10], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 12,040 independent school districts with enrollment populations less than 50,000. *See also* tbl.4. Special-Purpose Local

(continued….)

populations of less than 50,000.[29] Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."[30]

10. *Wired Telecommunications Carriers.* The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks.[31] Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services.[32] By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.[33] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[34]

11. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[35] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[36] Of this number, 2,964 firms operated with fewer than 250 employees.[37] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 5,183 providers that reported they were engaged in the provision of fixed local services.[38] Of these providers, the Commission estimates that 4,737

(Continued from previous page)
Governments by State Census Years 1942 to 2017 [CG1700ORG04], CG1700ORG04 Table Notes_Special Purpose Local Governments by State_Census Years 1942 to 2017.

[29] While the special purpose governments category also includes local special district governments, the 2017 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.

[30] This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,931) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (12,040), from the 2017 Census of Governments - Organizations tbls.5, 6 & 10.

[31] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[32] *Id.*

[33] *Id.*

[34] Fixed Local Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, and Other Local Service Providers. Local Resellers fall into another U.S. Census Bureau industry group and therefore data for these providers is not included in this industry.

[35] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[36] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[37] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[38] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

providers have 1,500 or fewer employees.[39] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

12. *Local Exchange Carriers* (*LECs*). Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include both incumbent and competitive local exchange service providers. Wired Telecommunications Carriers[40] is the closest industry with an SBA small business size standard.[41] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[42] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[43] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[44] Of this number, 2,964 firms operated with fewer than 250 employees.[45] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 5,183 providers that reported they were fixed local exchange service providers.[46] Of these providers, the Commission estimates that 4,737 providers have 1,500 or fewer employees.[47] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

13. *Incumbent Local Exchange Carriers (Incumbent LECs).* Neither the Commission nor the SBA have developed a small business size standard specifically for incumbent local exchange carriers. Wired Telecommunications Carriers[48] is the closest industry with an SBA small business size standard.[49] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[50] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[51] Of this number, 2,964 firms operated with fewer than

[39] *Id.*

[40] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[41] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[42] Fixed Local Exchange Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, Local Resellers, and Other Local Service Providers.

[43] *Id.*

[44] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[45] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[46] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[47] *Id.*

[48] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[49] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[50] *Id.*

[51] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311,

(continued….)

250 employees.[52] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 1,227 providers that reported they were incumbent local exchange service providers.[53] Of these providers, the Commission estimates that 929 providers have 1,500 or fewer employees.[54] Consequently, using the SBA's small business size standard, the Commission estimates that the majority of incumbent local exchange carriers can be considered small entities.

14. *Competitive Local Exchange Carriers (LECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include several types of competitive local exchange service providers.[55] Wired Telecommunications Carriers[56] is the closest industry with a SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[57] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[58] Of this number, 2,964 firms operated with fewer than 250 employees.[59] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 3,956 providers that reported they were competitive local exchange service providers.[60] Of these providers, the Commission estimates that 3,808 providers have 1,500 or fewer employees.[61] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

15. *Interexchange Carriers (IXCs).* Neither the Commission nor the SBA have developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications Carriers[62] is the closest industry with a SBA small business size standard.[63] The SBA small business size

(Continued from previous page)
https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[52] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[53] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf.

[54] *Id.*

[55] Competitive Local Exchange Service Providers include the following types of providers: Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, Local Resellers, and Other Local Service Providers.

[56] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[57] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[58] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[59] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[60] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[61] *Id.*

[62] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[64] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[65] Of this number, 2,964 firms operated with fewer than 250 employees.[66] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 151 providers that reported they were engaged in the provision of interexchange services. Of these providers, the Commission estimates that 131 providers have 1,500 or fewer employees.[67] Consequently, using the SBA's small business size standard, the Commission estimates that the majority of providers in this industry can be considered small entities.

16. *Cable System Operators (Telecom Act Standard)*. The Communications Act of 1934, as amended, contains a size standard for a "small cable operator," which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000.[68] For purposes of the Telecom Act Standard, the Commission determined that a cable system operator that serves fewer than 677,000 subscribers, either directly or through affiliates, will meet the definition of a small cable operator based on the cable subscriber count established in a 2001 Public Notice.[69] Based on industry data, only six cable system operators have more than 677, 000 subscribers.[70] Accordingly, the Commission estimates that the majority of cable system operators are small under this size standard. We note however, that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million.[71] Therefore, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

(Continued from previous page)

[63] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[64] *Id.*

[65] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[66] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[67] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf.

[68] 47 U.S.C. § 543(m)(2).

[69] *FCC Announces New Subscriber Count for the Definition of Small Cable Operator*, Public Notice, 16 FCC Rcd 2225 (CSB 2001) (*2001 Subscriber Count PN*). In this Public Notice, the Commission determined that there were approximately 67.7 million cable subscribers in the United States at that time using the most reliable source publicly available. *Id*. We recognize that the number of cable subscribers changed since then and that the Commission has recently estimated the number of cable subscribers to traditional and telco cable operators to be approximately 58.1 million. *See Communications Marketplace Report*, GN Docket No. 20-60, 2020 Communications Marketplace Report, 36 FCC Rcd 2945, 3049, para. 156 (2020) (*2020 Communications Marketplace Report*). However, because the Commission has not issued a public notice subsequent to the *2001 Subscriber Count PN,* the Commission still relies on the subscriber count threshold established by the *2001 Subscriber Count PN* for purposes of this rule. *See* 47 CFR § 76.901(e)(1).

[70] S&P Global Market Intelligence, S&P Capital IQ Pro, *Top Cable MSOs 12/21Q (*last visited May 26, 2022); S&P Global Market Intelligence, Multichannel Video Subscriptions, Top 10 (April 2022).

[71] The Commission does receive such information on a case-by-case basis if a cable operator appeals a local franchise authority's finding that the operator does not qualify as a small cable operator pursuant to § 76.901(e) of the Commission's rules. *See* 47 CFR § 76.910(b).

17. *Other Toll Carriers*. Neither the Commission nor the SBA has developed a definition for small businesses specifically applicable to Other Toll Carriers. This category includes toll carriers that do not fall within the categories of interexchange carriers, operator service providers, prepaid calling card providers, satellite service carriers, or toll resellers. Wired Telecommunications Carriers[72] is the closest industry with a SBA small business size standard.[73] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[74] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[75] Of this number, 2,964 firms operated with fewer than 250 employees.[76] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 115 providers that reported they were engaged in the provision of other toll services.[77] Of these providers, the Commission estimates that 113 providers have 1,500 or fewer employees.[78] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

18. *Wireless Telecommunications Carriers (except Satellite)*. This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves.[79] Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services.[80] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[81] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year.[82] Of that number, 2,837 firms employed fewer than 250 employees.[83] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 797 providers that reported they were engaged in the provision of wireless services.[84] Of these providers, the Commission estimates that 715 providers have 1,500 or fewer

---

[72] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[73] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111)..

[74] *Id.*

[75] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[76] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[77] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[78] *Id.*

[79] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[80] *Id.*

[81] *See* 13 CFR § 121.201, NAICS Code 517312 (as of 10/1/22, NAICS Code 517112).

[82] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[83] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[84] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

employees.[85] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

19. *Satellite Telecommunications.* This industry comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[86] Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $35 million or less in annual receipts as small.[87] U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year.[88] Of this number, 242 firms had revenue of less than $25 million.[89] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 71 providers that reported they were engaged in the provision of satellite telecommunications services.[90] Of these providers, the Commission estimates that approximately 48 providers have 1,500 or fewer employees.[91] Consequently using the SBA's small business size standard, a little more than of these providers can be considered small entities.

20. *Local Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Local Resellers. Telecommunications Resellers is the closest industry with a SBA small business size standard.[92] The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households.[93] Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[94] Mobile virtual network operators (MVNOs) are included in this industry.[95] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[96] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[97] Of that number, 1,375

[85] *Id.*

[86] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications,"* https://www.census.gov/naics/?input=517410&year=2017&details=517410.

[87] *See* 13 CFR § 121.201, NAICS Code 517410.

[88] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517410, https://data.census.gov/cedsci/table?y=2017&n=517410&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[89] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[90] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[91] *Id.*

[92] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[93] *Id.*

[94] *Id*.

[95] *Id*.

[96] *See* 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

firms operated with fewer than 250 employees.[98] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 293 providers that reported they were engaged in the provision of local resale services.[99] Of these providers, the Commission estimates that 289 providers have 1,500 or fewer employees.[100] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

21. *Toll Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Toll Resellers. Telecommunications Resellers[101] is the closest industry with an SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[102] Mobile virtual network operators (MVNOs) are included in this industry.[103] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[104] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[105] Of that number, 1,375 firms operated with fewer than 250 employees.[106] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 518 providers that reported they were engaged in the provision of toll services.[107] Of these providers, the Commission estimates that 495 providers have 1,500 or fewer employees.[108] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

22. *Prepaid Calling Card Providers*. Neither the Commission nor the SBA has developed a small business size standard specifically for prepaid calling card providers. Telecommunications

(Continued from previous page)

[97] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[98] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[99] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[100] *Id.*

[101] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[102] *Id.*

[103] *Id*.

[104] *See* 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[105] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[106] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[107] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[108] *Id.*

Resellers[109] is the closest industry with a SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[110] Mobile virtual network operators (MVNOs) are included in this industry.[111] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[112] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[113] Of that number, 1,375 firms operated with fewer than 250 employees.[114] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 58 providers that reported they were engaged in the provision of payphone services.[115] Of these providers, the Commission estimates that 57 providers have 1,500 or fewer employees.[116] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

23. *All Other Telecommunications.* This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[117] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[118] Providers of Internet services (e.g. dial-up ISPs) or voice over Internet protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry.[119] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small.[120] U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[121] Of those firms, 1,039 had revenue of less than $25 million.[122] Based

[109] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[110] *Id.*

[111] *Id*.

[112] *See* 13 CFR § 121.201, NAICS Code 517911(as of 10/1/22, NAICS Code 517121).

[113] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[114] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[115] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021),

https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[116] *Id.*

[117] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517919 All Other Telecommunications,*" https://www.census.gov/naics/?input=517919&year=2017&details=517919.

[118] *Id.*

[119] *Id*.

[120] *See* 13 CFR § 121.201, NAICS Code 517919 (as of 10/1/22, NAICS Code 517810).

[121] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517919,

(continued….)

on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

E. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

24. The *Sixth Report and Order* requires providers to meet certain obligations. These changes affect small and large companies equally and apply equally to all the classes of regulated entities identified above. Specifically, the *Sixth Report and Order* adopts a limited intermediate provider authentication requirement. It requires a non-gateway intermediate provider that receives an unauthenticated SIP call directly from an originating provider to authenticate the call.[123] The requirement will arise in limited circumstances—where the originating provider failed to comply with their own authentication obligation, or where the call is sent directly to an intermediate provider from the limited subset of originating providers that lack an authentication obligation. Indeed, if the first intermediate provider in the call path implements contractual provisions with its upstream originating providers stating that it will only accept authenticated traffic, it will completely avoid the need to authenticate calls.[124] Non-gateway intermediate providers that are subject to the authentication obligation have the flexibility to assign the level of attestation appropriate to the call based on the current version of the standards and the call information available.[125]

25. The *Sixth Report and Order* also requires all providers to take "reasonable steps" to mitigate illegal robocalls.[126] The new classes of providers subject to the "reasonable steps" standard are not required to implement specific measures to meet that standard, but providers' programs must include detailed practices that can reasonably be expected to significantly reduce the carrying, processing, or origination of illegal robocalls.[127] In addition, all providers must implement a robocall mitigation program and comply with the practices that its program requires.[128] The providers must also commit to respond fully to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocalls.[129]

26. All providers must submit a certification and robocall mitigation plan to the Robocall Mitigation Database regardless of whether they are required to implement STIR/SHAKEN, including providers without the facilities necessary to implement STIR/SHAKEN.[130] The robocall mitigation plan must describe the specific "reasonable steps" that the provider has taken to avoid, as applicable, the origination, carrying, or processing of illegal robocall traffic.[131] The *Sixth Report and Order* also requires

(Continued from previous page)
https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[122] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[123] *Sixth Report and Order* Section III.A.1.

[124] *Id.*

[125] *Id.* Section III.A.2.

[126] *Id.* Section III.B.1.

[127] *Id.*

[128] *Id.*

[129] *Id.*

[130] *Id.* Section III.B.2.

[131] *Id.*

providers to "describe with particularity" certain mitigation techniques in their robocall mitigation plans. Specifically, (1) voice service providers must describe how they are complying with their existing obligation to take affirmative effective measures to prevent new and renewing customers from originating illegal calls; (2) non-gateway intermediate providers and voice service providers must describe any "know-your-upstream provider" procedures; and (3) all providers must describe any call analytics systems used to identify and block illegal traffic. To comply with the new requirements to describe their "new and renewing customer" and "know-your-upstream provider" procedures, providers must describe any contractual provisions with end-users or upstream providers designed to mitigate illegal robocalls.[132]

27. All providers with new filing obligations must submit a certification to the Robocall Mitigation Database that includes the following baseline information:

(1) whether the provider has fully, partially, or not implemented the STIR/SHAKEN authentication framework in the IP portions of its network;

(2) the provider's business name(s) and primary address;

(3) other business name(s) in use by the provider;

(4) all business names previously used by the provider;

(5) whether the provider is a foreign service provider;

(6) the name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues.[133]

28. Certifications and robocall mitigations plans must be submitted in English or with certified English translation, and providers with new filing obligations must update any submitted information within 10 business days.[134]

29. The Sixth *Report and Order* also adopts rules requiring providers to submit additional information in their Robocall Mitigation certifications. Specifically, (1) all providers must submit additional information regarding their role(s) in the call chain; (2) all providers asserting they do not have an obligation to implement STIR/SHAKEN must include more detail regarding the basis of that assertion; (3) all providers must certify that they have not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action; (4) all providers must submit information regarding prior enforcement actions; and (5) all filers must submit their OCN if they have one.[135] Submissions may be made confidentially, consistent with our existing confidentiality rules.[136]

30. The *Sixth Report and Order* requires downstream providers to block traffic received from a non-gateway intermediate provider that is not listed in the Robocall Mitigation Database, either because the provider did not file or their certification was removed as part of an enforcement action.[137] After receiving notice from the Commission that a provider has been removed from the Robocall Mitigation Database, downstream providers must block all traffic from the identified provider within two business days.[138]

---

[132] *Id.*

[133] *Id.*

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] *Id.*

[138] *Id.* Section III.C.2.

F. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

31. The RFA requires an agency to describe any significant alternatives that it has considered in reaching its approach, which may include the following four alternatives, among others: (1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for small entities; (3) the use of performance, rather than design, standards; and (4) an exemption from coverage of the rule, or any part thereof, for small entities.[139]

32. Generally, the decisions we made in the *Sixth Report and Order* apply to all providers, and do not impose unique burdens or benefits on small providers. We took several steps to minimize the economic impact of the rules adopted in today's *Sixth Report and Order* on small entities.

33. The *Sixth Report and Order* imposes a limited intermediate provider authentication obligation that requires the first non-gateway intermediate provider in the call chain to authenticate unauthenticated calls received directly from an originating provider.[140] Limiting the application of the authentication obligation to first non-gateway intermediate providers helps reduce the burden on intermediate providers, including small providers, and minimizes the potential costs associated with a broader authentication requirement for all intermediate providers that were identified in the record.[141]

34. We also allowed flexibility where appropriate to ensure that providers, including small providers, can determine the best approach for compliance based on the needs of their networks. For example, non-gateway intermediate providers have the flexibility to assign the level of attestation appropriate to the call based on the applicable level of the standards and the available call information.[142] Additionally, the new classes of providers subject to the "reasonable steps" standard have the flexibility to determine which measures to use to mitigate illegal robocall traffic on their networks.[143] In reaching this approach, we considered and declined to adopt a "gross negligence" standard for evaluating whether a mitigation program is sufficient.[144] We also declined to adopt a heightened mitigation obligation solely for VoIP providers in order to ensure that the obligation applies to providers regardless of the technology used to transmit calls.[145]

35. The Sixth *Report and Order* also grants an indefinite STIR/SHAKEN implementation extension to satellite providers that are small voice service providers and use NANP numbers to originate calls.[146]

G. Report to Congress

36. The Commission will send a copy of the *Sixth Report and Order*, including this FRFA, in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act.[147] In addition, the Commission will send a copy of the *Sixth Report and Order*, including

[139] 5 U.S.C. § 603.

[140] *Sixth Report and Order* Section III.A.1.

[141] *Id.*

[142] *Id.* Section III.A.2.

[143] *Id.* Section III.B.1.

[144] *Id.*

[145] *Id.*

[146] *Id.* Section III.D.

[147] 5 U.S.C. § 801(a)(1)(A).

this FRFA, to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the *Sixth Report and Order* (or summaries thereof) will also be published in the Federal Register.[148]

[148] *See id*. § 604(b).

APPENDIX C

Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Commission has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities by the policies and rules proposed in this Further Notice of Proposed Rulemaking (*Sixth Further Notice or Further Notice*). The Commission requests written public comments on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments provided on the first page of the Further Notice. The Commission will send a copy of the Further Notice, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[2] In addition, the Further Notice and IRFA (or summaries thereof) will be published in the Federal Register.[3]

A. Need for, and Objectives of, the Proposed Rules

2. In order to continue the Commission's work of protecting American consumers from illegal calls, the *Sixth Further Notice* seeks comment on the use of third-party caller ID authentication solutions and whether any *changes* should be made to the Commission's rules to permit, prohibit, or limit their use.[4] It also seeks comment on whether to eliminate the STIR/SHAKEN implementation extension for voice service providers that cannot obtain an SPC token.[5]

B. Legal Basis

3. The *Sixth Further Notice* proposes to find authority largely under those provisions through which it has previously adopted rules. Specifically, the *Sixth Further Notice* proposes to find authority under section 251(e) of the Communications Act of 1934, as amended, the Truth in Caller ID Act, and the TRACED Act.[6] The *Sixth Further Notice* solicits comment on these proposals.[7]

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

4. The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules and by the rule revisions on which the Notice seeks comment, if adopted.[8] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[9] In addition, the term "small business" has the same meaning as the term "small-business concern" under the Small Business Act.[10] A "small-business concern" is one which: (1) is independently

[1] *See* 5 U.S.C. § 603. The RFA, *see* 5 U.S.C. § 601-612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[2] *See* 5 U.S.C. § 603(a).

[3] *See id*.

[4] *Sixth Further Notice* Section IV.A.

[5] *Id.* Section IV.B.

[6] *Id.* Section IV.C.

[7] *Id.*

[8] *See* 5 U.S.C. § 603(b)(3).

[9] *See id*. § 601(6).

[10] *Id*. § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and (continued….)

owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[11]

5. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein.[12] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[13] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 32.5 million businesses.[14]

6. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[15] The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations.[16] Nationwide, for tax year 2020, there were approximately 447,689 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.[17]

7. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[18] U.S. Census Bureau data from the 2017 Census of Governments[19] indicate there were 90,075 local governmental jurisdictions consisting of general

(Continued from previous page)
publishes such definition(s) in the Federal Register."

[11] *See* 15 U.S.C. § 632.

[12] *See* 5 U.S.C. § 601(3)-(6).

[13] *See* SBA, Office of Advocacy, Frequently Asked Questions, "What is a small business?," https://cdn.advocacy.sba.gov/wp-content/uploads/2021/11/03093005/Small-Business-FAQ-2021.pdf. (Nov 2021).

[14] *Id*.

[15] *See* 5 U.S.C. § 601(4).

[16] The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number small organizations in this small entity description. S*ee* Annual Electronic Filing Requirement for Small Exempt Organizations — Form 990-N (e-Postcard), 'Who must file."

https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

[17] *See* Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO BMF data for businesses for the tax year 2020 with revenue less than or equal to $50,000, for Region 1-Northeast Area (58,577), Region 2-Mid-Atlantic and Great Lakes Areas (175,272), and Region 3-Gulf Coast and Pacific Coast Areas (213,840) that includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

[18] *See* 5 U.S.C. § 601(5).

[19] *See* 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* Census of Governments, https://www.census.gov/programs-surveys/cog/about.html.

purpose governments and special purpose governments in the United States.[20] Of this number there were 36,931 general purpose governments (county[21], municipal and town or township[22]) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts[23] with enrollment populations of less than 50,000.[24] Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."[25]

8. *Wired Telecommunications Carriers.* The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks.[26] Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services.[27] By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.[28] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[29]

---

[20] *See* U.S. Census Bureau, 2017 Census of Governments – Organization Table 2. Local Governments by Type and State: 2017 [CG1700ORG02], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). *See also* tbl.2. CG1700ORG02 Table Notes_Local Governments by Type and State_2017.

[21] *See id*. at tbl.5. County Governments by Population-Size Group and State: 2017 [CG1700ORG05], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

[22] *See id*. at tbl.6. Subcounty General-Purpose Governments by Population-Size Group and State: 2017 [CG1700ORG06], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 18,729 municipal and 16,097 town and township governments with populations less than 50,000.

[23] *See id.* at tbl.10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2017 [CG1700ORG10], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 12,040 independent school districts with enrollment populations less than 50,000. *See also* tbl.4. Special-Purpose Local Governments by State Census Years 1942 to 2017 [CG1700ORG04], CG1700ORG04 Table Notes_Special Purpose Local Governments by State_Census Years 1942 to 2017.

[24] While the special purpose governments category also includes local special district governments, the 2017 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.

[25] This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,931) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (12,040), from the 2017 Census of Governments - Organizations tbls.5, 6 & 10.

[26] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[27] *Id*.

[28] *Id*.

[29] Fixed Local Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, and Other Local Service Providers. Local Resellers fall into another U.S. Census Bureau industry group and therefore data for these providers is not included in this industry.

9. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[30] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[31] Of this number, 2,964 firms operated with fewer than 250 employees.[32] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 5,183 providers that reported they were engaged in the provision of fixed local services.[33] Of these providers, the Commission estimates that 4,737 providers have 1,500 or fewer employees.[34] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

10. *Local Exchange Carriers (LECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include both incumbent and competitive local exchange service providers. Wired Telecommunications Carriers[35] is the closest industry with an SBA small business size standard.[36] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[37] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[38] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[39] Of this number, 2,964 firms operated with fewer than 250 employees.[40] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 5,183 providers that reported they were fixed local exchange service providers.[41] Of these providers, the Commission estimates that 4,737 providers have 1,500 or

[30] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/12, NAICS Code 517111).

[31] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[32] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[33] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[34] *Id*.

[35] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[36] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[37] Fixed Local Exchange Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, Local Resellers, and Other Local Service Providers.

[38] *Id*.

[39] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[40] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[41] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

fewer employees.[42] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

11. *Incumbent Local Exchange Carriers (Incumbent LECs).* Neither the Commission nor the SBA have developed a small business size standard specifically for incumbent local exchange carriers. Wired Telecommunications Carriers[43] is the closest industry with an SBA small business size standard.[44] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[45] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[46] Of this number, 2,964 firms operated with fewer than 250 employees.[47] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 1,227 providers that reported they were incumbent local exchange service providers.[48] Of these providers, the Commission estimates that 929 providers have 1,500 or fewer employees.[49] Consequently, using the SBA's small business size standard, the Commission estimates that the majority of incumbent local exchange carriers can be considered small entities.

12. *Competitive Local Exchange Carriers (LECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include several types of competitive local exchange service providers.[50] Wired Telecommunications Carriers[51] is the closest industry with an SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[52] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[53] Of this number, 2,964 firms operated with fewer than

[42] *Id.*

[43] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[44] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[45] *Id.*

[46] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[47] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[48] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf.

[49] *Id.*

[50] Competitive Local Exchange Service Providers include the following types of providers: Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, Local Resellers, and Other Local Service Providers.

[51] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[52] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[53] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

250 employees.[54] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 3,956 providers that reported they were competitive local exchange service providers.[55] Of these providers, the Commission estimates that 3,808 providers have 1,500 or fewer employees.[56] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

13. We have included small incumbent LECs in this present RFA analysis. As noted above, a "small business" under the RFA is one that, *inter alia*, meets the pertinent small-business size standard (e.g., a telephone communications business having 1,500 or fewer employees) and "is not dominant in its field of operation."[57] The SBA's Office of Advocacy contends that, for RFA purposes, small incumbent LECs are not dominant in their field of operation because any such dominance is not "national" in scope.[58] We have therefore included small incumbent LECs in this RFA analysis, although we emphasize that this RFA action has no effect on Commission analyses and determinations in other, non-RFA contexts.

14. *Interexchange Carriers (IXCs).* Neither the Commission nor the SBA have developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications Carriers[59] is the closest industry with a SBA small business size standard.[60] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[61] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[62] Of this number, 2,964 firms operated with fewer than 250 employees.[63] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 151 providers that reported they were engaged in the provision of interexchange services. Of these providers, the Commission estimates that 131 providers have 1,500 or fewer employees.[64] Consequently, using the SBA's small business size standard, the Commission estimates that the majority of providers in this industry can be considered small entities.

---

[54] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[55] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[56] *Id*.

[57] 5 U.S.C. § 601(3).

[58] Letter from Jere W. Glover, Chief Counsel for Advocacy, SBA, to William E. Kennard, Chairman, FCC (filed May 27, 1999). The Small Business Act contains a definition of "small business concern," which the RFA incorporates into its own definition of "small business." 15 U.S.C. § 632(a); 5 U.S.C. § 601(3). SBA regulations interpret "small business concern" to include the concept of dominance on a national basis. 13 CFR § 121.102(b).

[59] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[60] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[61] *Id*.

[62] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[63] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[64] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf.

15. *Cable System Operators (Telecom Act Standard)*. The Communications Act of 1934, as amended, contains a size standard for a "small cable operator," which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000."[65] For purposes of the Telecom Act Standard, the Commission determined that a cable system operator that serves fewer than 677,000 subscribers, either directly or through affiliates, will meet the definition of a small cable operator based on the cable subscriber count established in a 2001 Public Notice.[66] Based on industry data, only six cable system operators have more than 677,000 subscribers.[67] Accordingly, the Commission estimates that the majority of cable system operators are small under this size standard. We note however, that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million.[68] Therefore, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

16. *Other Toll Carriers*. Neither the Commission nor the SBA has developed a definition for small businesses specifically applicable to Other Toll Carriers. This category includes toll carriers that do not fall within the categories of interexchange carriers, operator service providers, prepaid calling card providers, satellite service carriers, or toll resellers. Wired Telecommunications Carriers[69] is the closest industry with a SBA small business size standard.[70] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[71] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[72] Of this number, 2,964 firms operated with fewer than 250 employees.[73] Additionally, based on

---

[65] 47 U.S.C. § 543(m)(2).

[66] *FCC Announces New Subscriber Count for the Definition of Small Cable Operator*, Public Notice, 16 FCC Rcd 2225 (CSB 2001) (*2001 Subscriber Count PN*). In this Public Notice, the Commission determined that there were approximately 67.7 million cable subscribers in the United States at that time using the most reliable source publicly available. *Id*. We recognize that the number of cable subscribers changed since then and that the Commission has recently estimated the number of cable subscribers to traditional and telco cable operators to be approximately 58.1 million. *See Communications Marketplace Report*, GN Docket No. 20-60, 2020 Communications Marketplace Report, 36 FCC Rcd 2945, 3049, para. 156 (2020) (*2020 Communications Marketplace Report*). However, because the Commission has not issued a public notice subsequent to the *2001 Subscriber Count PN,* the Commission still relies on the subscriber count threshold established by the *2001 Subscriber Count PN* for purposes of this rule. *See* 47 CFR § 76.901(e)(1).

[67] S&P Global Market Intelligence, S&P Capital IQ Pro, *Top Cable MSOs 12/21Q (*last visited May 26, 2022); S&P Global Market Intelligence, Multichannel Video Subscriptions, Top 10 (April 2022).

[68] The Commission does receive such information on a case-by-case basis if a cable operator appeals a local franchise authority's finding that the operator does not qualify as a small cable operator pursuant to § 76.901(e) of the Commission's rules. *See* 47 CFR § 76.910(b).

[69] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[70] *See* 13 CFR § 121.201, NAICS Code 517311.

[71] *Id.*

[72] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[73] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 115 providers that reported they were engaged in the provision of other toll services.[74] Of these providers, the Commission estimates that 113 providers have 1,500 or fewer employees.[75] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

17. *Wireless Telecommunications Carriers (except Satellite).* This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves.[76] Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services.[77] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[78] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year.[79] Of that number, 2,837 firms employed fewer than 250 employees.[80] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 797 providers that reported they were engaged in the provision of wireless services.[81] Of these providers, the Commission estimates that 715 providers have 1,500 or fewer employees.[82] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

18. *Satellite Telecommunications.* This industry comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[83] Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $35 million or less in annual receipts as small.[84] U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year.[85] Of this number, 242 firms had revenue of less than

[74] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[75] *Id.*

[76] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[77] *Id*.

[78] *See* 13 CFR § 121.201, NAICS Code 517312 (as of 10/1/22, NAICS Code 517112).

[79] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[80] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[81] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[82] *Id*.

[83] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications,"* https://www.census.gov/naics/?input=517410&year=2017&details=517410.

[84] *See* 13 CFR § 121.201, NAICS Code 517410.

[85] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517410, https://data.census.gov/cedsci/table?y=2017&n=517410&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

$25 million.[86] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 71 providers that reported they were engaged in the provision of satellite telecommunications services.[87] Of these providers, the Commission estimates that approximately 48 providers have 1,500 or fewer employees.[88] Consequently using the SBA's small business size standard, a little more than of these providers can be considered small entities.

19. *Local Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Local Resellers. Telecommunications Resellers is the closest industry with a SBA small business size standard.[89] The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households.[90] Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[91] Mobile virtual network operators (MVNOs) are included in this industry.[92] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[93] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[94] Of that number, 1,375 firms operated with fewer than 250 employees.[95] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 293 providers that reported they were engaged in the provision of local resale services.[96] Of these providers, the Commission estimates that 289 providers have 1,500 or fewer employees.[97] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

20. *Toll Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Toll Resellers. Telecommunications Resellers[98] is the closest industry with a SBA small business size standard. The Telecommunications Resellers industry comprises

[86] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[87] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[88] *Id*.

[89] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] *See* 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[94] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[95] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[96] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[97] *Id*.

[98] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[99] Mobile virtual network operators (MVNOs) are included in this industry.[100] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[101] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[102] Of that number, 1,375 firms operated with fewer than 250 employees.[103] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 518 providers that reported they were engaged in the provision of toll services.[104] Of these providers, the Commission estimates that 495 providers have 1,500 or fewer employees.[105] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

21. *Prepaid Calling Card Providers.* Neither the Commission nor the SBA has developed a small business size standard specifically for prepaid calling card providers. Telecommunications Resellers[106] is the closest industry with a SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[107] Mobile virtual network operators (MVNOs) are included in this industry.[108] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[109] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[110] Of that number, 1,375 firms operated with fewer than 250 employees.[111]

---

[99] *Id*.

[100] *Id.*

[101] *See* 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[102] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[103] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[104] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[105] *Id*.

[106] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[107] *Id*.

[108] *Id.*

[109] *See* 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[110] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[111] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 58 providers that reported they were engaged in the provision of payphone services.[112] Of these providers, the Commission estimates that 57 providers have 1,500 or fewer employees.[113] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

22. *All Other Telecommunications.* This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[114] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[115] Providers of Internet services (e.g. dial-up ISPs) or voice over Internet protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry.[116] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small.[117] U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[118] Of those firms, 1,039 had revenue of less than $25 million.[119] Based on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

23. The *Sixth Further Notice* seeks comment on imposing several obligations on various providers, many of whom may be small entities. Specifically, the *Sixth Further Notice* seeks comment on the types of third-party authentication solutions being used by providers and the nature of any agreements or relationships with third parties, including whether providers are entering into agreements with third parties to perform their authentication obligations under the Commission's rules and the ATIS technical standards.[120]

24. The *Sixth Further Notice* seeks comment on whether, and under what circumstances, a third party may authenticate calls on behalf of a provider with A- or B-level attestations consistent with the ATIS standards.[121] To the extent that commenters contend that third parties can meet the ATIS standards for signing calls with A- and B-level attestations, the *Sixth Further Notice* seeks comment on

[112] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[113] *Id*.

[114] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517919 All Other Telecommunications,*" https://www.census.gov/naics/?input=517919&year=2017&details=517919.

[115] *Id*.

[116] *Id.*

[117] *See* 13 CFR § 121.201, NAICS Code 517919 (as of 10/1/22, NAICS Code 517810).

[118] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517919, https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[119] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[120] *Sixth Further Notice* Section IV.A.

[121] Section IV.A.

the specific legal bases for that conclusion and the information that must be shared between originating providers and third parties for such attestation levels to be applied.[122] It also seeks comment on whether the Commission should condition any explicit authorization of third-party authentication solutions upon any particular restrictions or protections related to information sharing, including ensuring that third parties have the information needed to apply A- or B-level attestations consistent with the ATIS standards.[123]

25. The *Sixth Further Notice* further seeks comment on whether the Commission should amend its rules to explicitly permit third-party authentication and any limitations the Commission should place on any such authorization, including: (1) whether to limit authorization to scenarios akin to those described in the ATIS standards; (2) whether to limit authorization to the technical solutions described in the NANC's 2021 Small Providers Report; (3) whether to only permit third-party authentication if the third party signs the call using the provider's SPC token; (4) whether to require providers with the authentication obligation to make attestation-level determinations; and (5) whether to prohibit providers from certifying that they have implemented STIR/SHAKEN in the Robocall Mitigation Database unless their calls are singed with their own SPC token, whether directly or through a third-party.[124]

26. The *Sixth Further Notice* seeks comment on whether the Commission should change any other rules if certain third-party authentication practices are explicitly authorized.[125] In particular, it seeks comment on whether the Commission should require providers to explicitly identify certain additional information in their Robocall Mitigation Database certifications and plans, including: (1) any third-party solutions; (2) the identity of the third party providing the solution; and (3) any requirements the provider has imposed on the third party to ensure compliance with the requirements of the of the ATIS technical standards and Commission's rules, and any action taken by the provider to ensure compliance with those requirements.

27. The *Sixth Further Notice* seeks comment on whether there are any other compliance or enforcement measures that the Commission should adopt if it explicitly authorizes third-party authentication.[126] It also seeks comment on whether a rulemaking is necessary to address third-party authentication or if another procedural device would be appropriate.[127] To the extent that third-party caller ID authentication is explicitly authorized, the *Sixth Further Notice* seeks comment on whether the Commission should require providers that are not currently required to implement STIR/SHAKEN because they do not have the facilities necessary to do so or are subject to an implementation extension to engage a third-party authentication solution for the SIP calls they originate.[128]

28. Lastly, the *Sixth Further Notice* also seeks comment on whether to eliminate the STIR/SHAKEN implementation extension for providers that cannot obtain an SPC token.[129]

E. Steps Taken to Minimize the Significant Economic Impact on Small Entities and Significant Alternatives Considered

29. The RFA requires an agency to describe any significant alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): (1)

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] *Id.*

[126] *Id.*

[127] *Id.*

[128] *Id.*

[129] *Id.* Section IV.B.

the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rules for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities.[130]

30. The *Sixth Further Notice* seeks comment on the particular impacts that the proposed rules may have on small entities. In particular, it seeks comment regarding the different types of third-party authentication arrangements currently being employed by providers, the prevalence of each type of third-party authentication arrangement in the STIR/SHAKEN ecosystem, and any available data substantiating how effective they are at facilitating the authentication of caller ID information.[131]

31. The *Sixth Further Notice* seeks comment on whether third-party authentication providers are able to satisfy all or any of the ATIS standards, and whether the answer to such question is dependent on the nature of the relationship between the originating provider and the third party.[132]

32. The *Sixth Further Notice* seeks comment on the information that must be shared between originating providers and third parties for A- or B-level attestations to be applied and whether information sharing practices implicate any legal or public interest concerns.[133] It seeks comment on whether the Commission should condition any explicit authorization of third-party authentication practices upon providers ensuring that third parties have the information needed to apply A- or B-level attestations consistent with the ATIS standards.[134]

33. The *Sixth Further Notice* seeks comment on whether there is a distinction between scenarios in which third parties authenticate calls on behalf of a provider and the technical solutions described in the 2021 Small Providers Report produced by the NANC.[135] The *Sixth Further Notice* notes that the NANC described the technical solutions as a cost-effective means for providers—particularly small providers—to implement STIR/SHAKEN consistent with the ATIS standards, and sought comment on these solutions.[136] The *Sixth Further Notice* seeks comment on whether the Commission should limit any authorization of third-party authentication to the technical solutions described in the NANC's 2021 Small Provider Report.[137] It also seeks comment on only permitting third-party authentication if the third party signs the call using the provider's SPC token and prohibiting providers from certifying that they have implemented STIR/SHAKEN in the Robocall Mitigation Database unless their calls are signed with their own SPC token.[138] In so doing, it specifically seeks comment on whether the ability to obtain an SPC token is likely to present a barrier to providers' compliance with such a requirement.[139]

34. The *Sixth Further Notice* further seeks comment on the full range of potential benefits that could result from authorization of different third-party authentication arrangements, as well as the potential pitfalls of third-party authentication.[140] It also seeks comment on the specific costs that would

[130] 5 U.S.C. § 603(c)(1)-(4).

[131] *Sixth Further Notice* Section IV.A.

[132] *Id.*

[133] *Id.*

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] *Id.*

[138] *Id.*

[139] *Id.*

[140] *Id.*

be incurred and gains that would be realized if the Commission were to explicitly authorize or prohibit specific third-party authentication practices.[141] In addition, the *Sixth Further Notice* seeks comment on whether there are any other rules that the Commission would need to change if it were to explicitly authorize certain third-party authentication practices.[142] Moreover, if third-party caller ID authentication is explicitly permitted, the *Sixth Further Notice* seeks comment on whether to require providers that are not currently required to implement STIR/SHAKEN because they do not have the facilities necessary to do so or are subject to an implementation extension to engage a third-party authentication solution for the SIP calls they originate.[143]

35. Lastly, the *Sixth Further Notice* seeks comment on whether to eliminate the STIR/SHAKEN implementation for providers that cannot obtain an SPC token, as well as any benefits or drawbacks to retaining the extension.[144]

36. Small entities may provide input in these areas addressing, among other considerations, any particular implementation challenges faced by small entities. The Commission expects to evaluate the economic impact on small entities, as identified in comments filed in response to the *Further Notice* and this IRFA, in reaching its final conclusions and taking action in this proceeding.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

37. None.

[141] *Id.*

[142] *Id.*

[143] *Id.*

[144] *Id.* Section IV.B.